НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

КАФЕДРА СИСТЕМНОГО ПРОГРАМУВАННЯ І
СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

"На правах рукопису"
УДК_004.056_____

«До захисту допущено»
Завідувач кафедри

_____ В.П. Тарасенко
(підпис)

"___"_____2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 123 Комп'ютерна інженерія (Спеціалізовані комп'ютерні системи)
на тему: «**Модифікація методу стеганографії з використанням матриці судоку**»

Виконала: студентка ІІ курсу, групи КВ-63м
Липка Тетяна Богданівна _____
(підпис)

Науковий керівник доц. каф. СПСКС, к.т.н. Потапова К.Р. _____
(підпис)

Рецензент ст. викл. каф. ОТ ФІОТ Виноградов Ю.М. _____
(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – другий (магістерський)

Спеціальність 123 Комп'ютерна інженерія (Спеціалізовані комп'ютерні системи)
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.П. Тарасенко
(підпис) (ініціали, прізвище)
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Липці Тетяні Богданівні
(прізвище, ім'я, по батькові)

1. Тема дисертації «Модифікація методу стеганографії з використанням матриці судоку»,
науковий керівник дисертації Потапова К.Р., к.т.н, доц. каф. СПСКС. ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «22» березня 2018 р. № 986-С

2. Термін подання студентом дисертації 11 травня 2018 р.

3. Об'єктом дослідження є процес приховування інформації у зображеннях

4. Предметом дослідження є стеганографічні методи приховування графічної інформації з використанням матриці судоку.

5. Перелік завдань, які потрібно розробити:
- дослідити методи стеганографії та їх модифікації;
- провести аналіз спотворення та оптимального використання стего-контейнера;
- формалізувати вимоги до вибору стего-контейнера;
- розробити покращений метод приховування графічної інформації з використанням матриці судоку;
- дослідити можливість поширення даного методу на будь-які типи даних;
- дослідити його стеганографічну стійкість;
- провести аналіз еквівалентних перетворень матриць судоку;
- на основі запропонованих методів розробити програмне забезпечення з метою їх верифікації.

- розробити схему застосування модифікованого методу стеганографії;
- проаналізувати результати роботи представленого методу.

6. Орієнтовний перелік ілюстративного матеріалу:
- Алгоритм перевірки правильності судоку матриці. Схема алгоритму.
- Генерація стегоключа за паролем. Схема алгоритму.
- Алгоритм шифрування. Схема алгоритму.
- Алгоритм дешифрування. Схема алгоритму.
- Пошук найближчої точки в матриці судоку. Схема алгоритму.
- Перевірка значення в матриці судоку. Схема алгоритму.

7. Орієнтовний перелік публікацій:
- Тези доповідей на щорічних конференціях «Прикладна математика та комп'ютинг».

8. Дата видачі завдання 5 вересня 2016 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1.	Ґрунтовне ознайомлення з предметною галуззю	16.12.2016	
2.	Визначення структури магістерської дисертації; вивчення літератури, пошук додаткової літератури, патентний пошук	03.04.2016	
3.	Робота над першим розділом магістерської дисертації; проведення наукового дослідження	15.05.2017	
4.	Проведення наукового дослідження; робота над другим розділом магістерської дисертації; розроблення програмного забезпечення	20.12.2017	
5.	Проведення наукового дослідження; робота над статтями за результатами наукового дослідження	15.03.2018	
6.	Проведення наукового дослідження; робота над третім і четвертим розділами магістерської дисертації; підготовка матеріалів доповіді на конференції.	01.04.2018	
7.	Завершення роботи над основною частиною магістерської дисертації; підготовка ілюстративного матеріалу. Оформлення текстової і графічної частини магістерської дисертації.	20.04.2018	
8.	Попередній розгляд магістерської дисертації на кафедрі	26.04.2018	

Студент _____ Липка Т.Б. _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Потапова К.Р. _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Актуальність теми. Розвиток глобальної мережі Інтернет та поширення її використання сприяє збільшенню обсягів інформації, що передається, обробляється та зберігається. Використовуючи можливості та ресурси мережі Інтернет, можна організувати канал зв'язку, наприклад, з дипломатичними установами, що знаходяться на території іноземних держав. Скритність передачі інформації по такому каналу буде забезпечуватися стенографічними засобами захисту. Основна відмінність стеганографії від інших методів захисту інформації полягає саме у приховуванні факту існування секретного повідомлення в іншому, такому, що не привертає уваги об'єкті – контейнері, використовуючи для цього особливості побудови самого контейнера та властивості органів сприйняття людини.

Аналіз останніх досліджень і публікацій показав, що найбільшу популярність в комп'ютерній стеганографії здобули методи, що використовують в ролі контейнера зображення. Тому було вивчено і запропоновано модифікацію одного з них - методу стеганографії з використанням матриці судоку.

Проведений аналіз також показав, що однією з ключових проблем стеганографії є питання оптимального використання стегоконтейнера, оскільки потреба у передачі даних великого обсягу виникає частіше, ніж потреба у передачі даних невеликого обсягу. При роботі з даними великого обсягу важливим завданням є прискорення процесів шифрування, дешифрування інформації.

Часто сучасні стеганографічні методи використовують великі ключі, що заставляє користувачів зберігати їх у вигляді файлів. В такому випадку існує небезпека у викраденні цих файлів. Тому важливим завданням є приведення ключа до такого вигляду, щоб його можна було просто пам'ятати.

Об’єктом дослідження є процеси приховування інформації у зображення.

Предметом дослідження є стеганографічні методи приховування графічної інформації з використанням матриці судоку.

Метою даної роботи є покращення деяких якісних показників методу стеганографії з використанням матриці судоку.

Показниками, що покращуються є:

1. Пропускна здатність - кількість бітів секретного повідомлення, які можуть бути передані за допомогою даного методу в стегоконтейнері фіксованого розміру.

2. Складність вбудовування і вилучення - кількість стандартних операцій, які необхідно виконати для вбудовування і виявлення секретного повідомлення.

Методи дослідження. В роботі використовуються методи наукової абстракції, аналізу і синтезу (при розкритті теоретичних положень та формулюванні категоріального апарату), порівняння (для встановлення переваг та недоліків різних методів стеганографії), формалізації (для опису вимог до стегоконтейнера), емпіричні (для оцінки спотворень стегоконтейнера) та методи системного підходу.

Наукова новизна. Запропоновано модифікований метод стеганографії з використанням матриці судоку, який відрізняється від відомих покращенням якісних показників стеганосистеми - пропускної здатності та складності вбудовування і вилучення секретного повідомлення.

Практична цінність отриманих в роботі результатів полягає в розробці покращеного методу стеганографії, розробці програмних засобів для приховування зображень на основі запропонованих модифікацій.

Також, в даній роботі запропоновано спосіб генерації стегоключа (матриці судоку) за паролем, що дозволяє істотно спростити користувачеві

використання даного методу стеганографії, уникаючи необхідності зберігання ключів у вигляді файлів.

Таким чином, запропонований метод та розроблене програмне забезпечення є комплексним вирішення задачі приховування даних, спрощують використання стегосистеми, мінімізовують можливості випадкової втрати ключа або цілеспрямованого взлому.

Апробація роботи. Основні положення і результати роботи були представлені на 20-тій міжнародній конференції "Системний аналіз та інформаційні технології" ("System Analysis and Information Technologies") SAIT 2018 (21–24 травня 2018 року, Київ, Україна) та на X науковій конференції магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2018 (21-23 березня 2018 року, Київ, Україна).

Структура та обсяг роботи. Магістерська дисертація складається з вступу, чотирьох розділів, висновків та додатків.

У вступі надано загальну характеристику роботи, виконано оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень, сформульовано мету і задачі досліджень, показано наукову новизну отриманих результатів і практичну цінність роботи, наведено відомості про апробацію результатів.

У першому розділі розглянуто основні поняття стеганографії, обґрунтовано актуальність використання стеганографії для вирішення сучасних задач, наведено класифікацію показників, що дають якісні та кількісні оцінки стегосистем; наведено завдання (прихована передача даних, цифрові підписи, водяні знаки) та сфери її застосування.

У другому розділі проаналізовано передумови поширеності стеганографії зображень; фізіологічні та психофізіологічні особливості зорової системи людини (ЗСЛ), що створюють підґрунтя для використання стеганографії цифрових зображень; розглянуто класифікацію методів комп'ютерної стеганографії; проаналізовано ПЗ для стеганографічного

приховування графічної інформації; обґрунтовано актуальність стеганографії та необхідність у вдосконаленні її методів; наведено перелік проблем сучасних методів комп'ютерної стеганографії.

У третьому розділі запропоновано модифікації методу стеганографії з використанням матриці судоку; досліджено ряд практичних проблем стеганографії і способи їх вирішення.

У четвертому розділі проаналізовано результати використання даного методу на практиці, наведено можливості подальшого розвитку даного методу; наведено оцінки помітності спотворень заповнених контейнерів.

У висновках проаналізовано отримані результати роботи.

У додатках наведено алгоритми: кодування та декодування секретних даних за допомогою модифікованого методу стеганографії, генерації матриці судоку за паролем, перевірки матриці судоку, пошуку найближчої точки матриці, значення в якій дорівнює заданому та алгоритм перевірки значення.

Робота виконана на 97 аркушах, містить 3 додатки та посилання на список використаних літературних джерел з 24 найменувань. У роботі наведено 36 рисунків та 2 таблиці.

Ключові слова: стеганографія, метод з використанням матриці судоку.

ABSTRACT

Theme urgency. The development and expansion of the global Internet network contributes to increasing the volume of information transmitted, processed and stored. Using the capabilities and resources of the Internet, you can arrange a communication channel, for example, with diplomatic establishments located in the territory of foreign countries. The secrecy of the transmission of information on such a channel will be provided by steganography. The main difference between steganography and other methods of information security is in concealing the existence of a secret message in another, such that it does not attract attention to the object-container, using for this purpose the features of building the container itself and the properties of human perception.

An analysis of recent researches and publications have shown that the most popular in computer steganography are the methods, which uses an image as the container. Therefore, it has been studied and proposed modification of one of them - the method of steganography using the sudoku matrix.

The analysis has also shown that one of the key issues of steganography is the question of optimal container usage, since the need for transmission of large amounts of data occurs more often than the need for the transmission of small amounts of data. When working with large amounts of data, an important task is to accelerate the processes of encryption, decryption of information.

Often, modern steganography techniques use large keys, which forces users to store them as files. In this case, there is a risk of theft of these files. Therefore, an important task is to bring the key in such a way that it can be just remembered.

Object of research are the processes of concealing information in the image.

Subject of research are steganography methods for concealing graphic information using the sudoku matrix.

Research objective: the improvement of some qualitative indicators of the steganography method using the sudoku matrix.

The improvement indicators are:

1. Channel capacity - the number of secret messages that can be transmitted using this method in a fixed-sized container.

2. The complexity of embedding and deletion is the number of standard operations that must be performed for embedding and detecting a secret data.

Research methods. The methods of scientific abstraction, analysis and synthesis, comparison (to establish the advantages and disadvantages of different steganography methods), formalization (for describing the requirements to the stegocontainer), empirical (for estimating the distortions of the container), and methods of the system approach are used in the research.

Scientific novelty. The modified method of steganography using sudoku puzzle which differs from the known by improvement of qualitative indicators of the stegosystem - the chanel capacity and the complexity of embedding and extracting the secret message.

Practical value of the obtained in the work of the results is to develop an improved method of steganography, the development of software to hide images based on the proposed modifications.

Also, in this paper a method for generating a key (matrix of sudoku) by a password has been proposed, which simplifies the user's use of this steganography method, avoiding the need to store the keys as files.

Thus, the proposed method and the software developed is a complex solution to the data hiding problem, simplifies the stegosystem usage, minimizes the possibility of accidental key loss or targeted hacking.

Approbation. The basic points and outcomes of the research have been presented and discussed at the 10nd scientific conference for students and postgraduates «Applied mathematics and computing» PMK-2018 (Kyiv,

March 21-23, 2018) as well as at the 20th International Conference "System Analysis and Information Technologies" SAIT-2018 (May 21-24, 2018, Kyiv, Ukraine).

Structure and content of the thesis. The master thesis consists of the introduction, four chapters, conclusions and appendixes.

The introduction provides a general description of the work, an assessment of the current state of the problem is performed, the relevance of the direction is substantiated researches, the purpose and tasks of researches are formulated, the scientific novelty of the results obtained and the practical value of the work are shown, information on the approbation of the results is given.

The first chapter deals with the basic concepts of steganography, substantiates the relevance of the use of steganography for solving modern problems, describes the classification of indicators that provide qualitative and quantitative estimates of stegosystems; goals are presented (hidden data transmission, digital fingerprints, stego watermarking) and application areas.

The second chapter analyzes the preconditions of the prevalence of steganography of images; physiological and psychophysiological features of the visual system of the person, which create the basis for the use of steganography of digital images; the classification of methods of computer steganography is considered; analyzed software for steganographic concealment of graphic information; substantiated the relevance of steganography and the need to improve its methods; The list of problems of modern methods of computer steganography is given.

In the third chapter modifications of the steganography method with the use of the sudoku matrix are proposed; A number of practical problems of steganography and methods of their solution are investigated.

In the fourth chapter, the results of the use of this method in practice are analyzed, the possibilities of further development of this method are given; Estimates of distortion of filled containers are presented.

In the conclusions the results of work are analyzed.

The appendices provide algorithms for encoding and decoding sensitive data using a modified steganography method, generating a sudoku matrix with a password, verifying the matrix of sudoku, searching the nearest matrix point, the value of which is equal to the given value, and the validation algorithm.

The thests is present in 97 pages, contains 3 attachments and a link to the list of used literary sources of 24 titles. The paper contains 36 images and 2 tables.

Key words: steganography, steganography using sudoku puzzle.

РЕФЕРАТ

Актуальность темы. Развитие глобальной сети Интернет и распространение ее использования способствует увеличению объемов информации, передаваемой и обрабатываемой. Используя возможности и ресурсы сети Интернет, можно организовать канал связи, например, с дипломатическими учреждениями, находящимися на территории иностранных государств. Скрытность передачи информации по такому каналу будет обеспечиваться стенографическими средствами защиты. Основное отличие стеганографии от других методов защиты информации заключается именно в сокрытии факта существования секретного сообщения в другом, таком, что не привлекает внимания объекте - контейнере, используя для этого особенности построения самого контейнера и свойства органов восприятия человека.

Анализ последних исследований і публикаций показал, что наибольшее популярность в компьютерной стеганографии получили методы, использующие в роли контейнера изображения. Поэтому было изучено і предложено модификацию одного из них - метода стеганографии с использованием матрицы судоку.

Проведенный анализ также показал, что одной из ключевых проблем стеганографии - вопрос оптимального использования стегоконтейнера, поскольку потребность в передаче данных большого объема возникает чаще, чем потребность в передаче данных небольшого объема. При работе с данным большого объема важной задачей является ускорение процессов шифрования, дешифрования информации.

Часто современные стеганографические методы используют большие ключи, что заставляет пользователей хранить их в виде файлов. В таком случае существует опасность в краже этих файлов. Поэтому важной задачей является приведение ключа к такому виду, чтобы его можно было просто помнить.

Объектом исследования являются процессы сокрытия информации в изображение.

Предметом исследования являются стеганографические методы сокрытия графической информации с использованием матрицы судоку.

Целью данной работы является улучшение некоторых качественных показателей метода стеганографии с использованием матрицы судоку.

Показателями, которые улучшаются являются:

1. Пропускная способность - количество бит секретного сообщения, которые могут быть переданы с помощью данного метода в стегоконтейнере фиксированного размера.

2. Сложность встраивания і извлечения - количество стандартных операций, которые необходимо выполнить для встраивания і обнаружения секретного сообщения.

Методы исследования. В работе используются методы научной абстракции, анализа и синтеза (при раскрытии теоретических положений и формулировке категориального аппарата), сравнение (для установки преимуществ и недостатков различных методов стеганографии), формализации (для описания требований к стегоконтейнеру), эмпирические (для оценки искажений стегоконтейнера) и методы системного подхода.

Научная новизна. Предложен модифицированный метод стеганографии с использованием матрицы судоку, который отличается от известных улучшением качественных показателей стеганосистемы - пропускной способности и сложности встраивания и извлечения секретного сообщения.

Практическая ценность полученных в работе результатов заключается в разработке улучшенного метода стеганографии, разработке

программных средств для сокрытия изображений на основе предложенных модификаций.

Также, в данной работе предложен способ генерации стегоключа (матрицы судоку) по паролю, что позволяет существенно упростить пользователю использование данного метода стеганографии, избегая необходимости хранения ключей в виде файлов.

Таким образом, предложенный метод и разработанное программное обеспечение являются комплексным решением задачи сокрытия данных, упрощают использование стегосистемы, минимизируют возможности случайной потери ключа или целенаправленного взлома.

Апробация работы. Основные положения и результаты работы были представлены на 20-ой международной конференции "Системный анализ и информационные технологии" ("System Analysis and Information Technologies") SAIT 2018 (21-24 мая 2018, Киев, Украина) и на X научной конференции магистрантов и аспирантов «Прикладная математика и компьютинг» ПМК-2018 (21-23 марта 2018 года, Киев, Украина).

Структура и объем работы. Магистерская диссертация состоит из введения, четырех разделов, выводов и приложений.

Во введении дано общая характеристика работы, выполнена оценка современного состояния проблемы, обоснована актуальность направления исследований, сформулированы цели и задачи исследований, показано научную новизну полученных результатов и практическую ценность работы, приведены сведения об апробации результатов.

В первом разделе рассмотрены основные понятия стеганографии, обоснована актуальность использования стеганографии для решения современных задач, приведена классификация показателей, дающих качественные и количественные оценки стегосистем; приведены задачи (скрытая передача данных, цифровые подписи, водяные знаки) и сферы ее применения.

Во втором разделе проанализированы предпосылки распространенности стеганографии изображений; физиологические и психофизиологические особенности зрительной системы человека (ЗСЛ), которые создают основу для использования стеганографии цифровых изображений; рассмотрена классификация методов компьютерной стеганографии; проанализированы ПО для стеганографического сокрытия графической информации; обоснована актуальность стеганографии и необходимость в совершенствовании ее методов; приведен перечень проблем современных методов компьютерной стеганографии.

В третьем разделе предложены модификации метода стеганографии с использованием матрицы судоку; исследован ряд практических проблем стеганографии и способы их решения.

В четвертом разделе проанализированы результаты использования данного метода на практике, приведены возможности дальнейшего развития данного метода; приведены оценки заметности искажений заполненных контейнеров.

В выводах проанализированы полученные результаты работы.

В приложениях приведены алгоритмы: кодирование и декодирование секретных данных с помощью модифицированного метода стеганографии, генерации матрицы судоку по паролю, проверки матрицы судоку, поиска ближайшей точки матрицы, значение в которой равна заданному и алгоритм проверки значения.

Работа выполнена на 97 листах, содержит 3 приложения и ссылки на список использованных литературных источников из 24 наименований. В работе приведены 36 рисунков и 2 таблицы.

Ключевые слова: стеганография, метод с использованием матрицы судоку.

ЗМІСТ

Перелік скорочень, умовних позначень, термінів

AD (скорочено від англ. Absolute Difference) – середня абсолютна різниця;

ASCII (скорочено від англ. American Standard Code for Information Interchange) – Американський стандартний код для інформаційного обміну;

BMP (Bitmap) – формат файлу зображень растрової графіки, в якому зображення зберігається у вигляді двовимірного масиву пікселів;

CLR (The Common Language Runtime) – це компонент пакету Microsoft .NET Framework, віртуальна машина, на якій виконуються всі мови платформи .NET Framework;

CMYK (скорочено від англ. Cyan, Magenta, Yellow, BlacK color) – субтрактивна колірна модель, що використовується у поліграфії, зазвичай при повноколірному друці;

GIF (скорочено від англ. Graphic Interchange Format) – популярний растровий формат графічних зображень, який здатний зберігати стиснені дані без втрати якості у форматі не більше 256 кольорів;

ICO (Windows icon) – формат для зберігання файлів значків;

IF (скорочено від англ. Image Fidelity) – якість зображення;

JPEG (скорочено від англ. Joint Photographic Expert Group) – растровий формат збереження;

MSE (скорочено від англ. Mean Square Error) – середньоквадратична похибка;

NAD (скорочено від англ. Normalized Average Absolute Difference) – нормована середня абсолютна різниця;

PNG (скорочено від англ. Portable Network Graphic) – растровий формат збереження графічної інформації, що використовує стиснення без втрат;

RGB (скорочено від англ. Red, Green, Blue) – адитивна колірна модель, що описує спосіб синтезу кольору, за якою червоне, зелене та синє світло

накладаються разом, змішуючись у різноманітні кольори, яка широко застосовується в техніці, що відтворює зображення за допомогою випромінення світла;

SNR (скорочено від англ. Signal Noise Ratio) – співвідношення «сигнал/шум»;

SVC (скорочено від англ. System Version Control) – система контролю версій;

TIFF (скорочено від англ. Tagged Image File Format) – один з базових універсальних форматів представлення високоякісних зображень, які використовуються у поліграфічній галузі;

WoW (World of Warcraft) – багатокористувацька рольова онлайн-гра;

YCbCr – сімейство колірних просторів;

БД – база даних;

ВЧ – високочастотний;

ЗСЛ – зорова система людини;

КС – комп’ютерна стеганографія;

НЗБ – найменш значущий біт;

НЧ – низькочастотний;

ПЗ – програмне забезпечення;

ППД – прихована передача даних;

ЦВЗ (СВЗ) – цифровий (стеганографічний) водяний знак;

ЦП – цифрові підписи.

ВСТУП

Проблема захисту інформації від несанкціонованого доступу вирішувалася в усі часи історії людства [1]. Як і колись, на сьогоднішній день двома основними шляхами вирішення цієї проблеми є криптографія та стеганографія.

Криптографічний захист – система зміни інформації з метою зробити її незрозумілою для «непосвячених» (приховати повідомлення, зашифрувавши його). Такий захист не є ідеальним, оскільки наявність шифрованого повідомлення привертає увагу, і зловмисник, побачивши криптографічно захищений файл, одразу може помітити факт розміщення в ньому секретної інформації. Використання криптографічних перетворень забезпечує конфіденційність, цілісність та унікальність інформації, яку передають. Конфіденційність інформації досягається шляхом її шифрування. Але доступні сучасні інформаційні технології відкривають також безліч нових можливостей і для зловмисників у галузі інформаційної безпеки, тому використання для захисту даних лише криптографічних засобів сьогодні не гарантує безпечного обміну даними в телекомунікаційних чи комп'ютерних мережах.[2]

Приховування ж самого факту наявності секретних даних при їх передачі, зберіганні або обробці є завданням стеганографії. При цьому завдання виявлення інформації стає не таким важливим і вирішується в більшості випадків стандартними криптографічними методами. Тобто, під приховуванням існування інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні наявності іншого (секретного) повідомлення, але й взагалі унеможливлення виникнення будь-яких підозр стосовно цього, оскільки в останньому випадку проблема інформаційної безпеки адресується стійкості криптографічного коду [1].

Процес стеганографічного приховування інформації здійснюється різними способами. Спільною рисою таких способів є те, що секретне повідомлення приховується в об'єкт, що не привертає увагу і потім відкрито

передається в мережі без будь-яких побоювань стосовно виявлення прихованої інформації сторонніми особами.

В основу методів стеганографії покладено принцип, що базується на використанні наявної психо-візуальної надлишковості даних потенційних контейнерів, оскільки фізіологічні можливості людини є обмеженими, а око людини подібне до низькочастотного фільтру, для якого непомітні спотворення у високочастотній області зображення. [2] Звукові дані містять надлишкову інформацію в часовій області, тому теж підходять для використання в ролі контейнера.

Саме тому вбудовування інформації відбувається шляхом її стеганографічного перетворення. Воно дозволяє передавати повідомлення шляхом вбудовування їх зазвичай у цифрові дані, що мають аналогову природу – відео, зображення, аудіозаписи та ін..[2] Вбудовування інформації в текстові чи виконувані файли є також можливим, але менш поширеним.

Найефективнішим способом забезпечення конфіденційності інформації є суміщене використання стеганографічних і криптографічних засобів.[3]

Як бачимо, стеганографія не замінює, а доповнює криптографію в процесі забезпечення інформаційної безпеки.

Тенденції розвитку засобів інформаційної комунікації, що спостерігаються зараз, сприяють значному збільшенню швидкості та обсягів передачі й обробки інформації, а також забезпеченню організації дистанційного доступу до глобальних інформаційних ресурсів та появі нових типів каналів зв'язку.[2] Характерною рисою сучасного суспільства є організація та ведення інформаційної діяльності. Інформація є важливою складовою життя сучасної людини. Одержання доступу до неї з появою глобальних комп’ютерних мереж значно спростилося. Але водночас така зручність та швидкість доступу суттєво підвищують загрозу несанкціонованого доступу до даних (при відсутності спеціальних засобів для захисту).

Останнім часом спостерігається значне збільшення кількості кібератак, зокрема спроб перехоплення конфіденційної інформації, яка передається засобами глобальних інформаційних мереж. [2]

Обмеження на використання криптографічних засобів у ряді країн світу та виникнення проблеми захисту прав власності на інформацію, представлену в цифровому вигляді зумовлюють популярність досліджень у сфері стеганографії. Сучасні стеганографічні методи дозволяють не лише приховано передавати дані (класичне завдання стеганографії – прихована передача даних (ППД)), але також успішно вирішувати завдання захисту інформації від несанкціонованого копіювання, завадостійкої автентифікації, відслідковування поширення даних мережами зв’язку, пошуку інформації в мультимедійних базах даних (БД) та ін.. [4]

Це дозволяє в межах традиційних інформаційних потоків або інформаційного середовища вирішувати важливі питання захисту інформації цілого ряду прикладних галузей. [4]

Наприклад, на комп'ютерні графічні зображення, аудіо продукцію, літературні твори (програми в тому числі) наноситься спеціальна мітка, що залишається невидимою для очей людини, але розпізнається спеціальним програмним забезпеченням. Ця мітка містить приховану інформацію, яка підтверджує авторство або факт наявності права власності. Ця прихована інформація повинна забезпечити захист інтелектуальної власності. В якості ключової інформації (секретне повідомлення) можна використовувати дані про автора, дату і місце народження твору, номера документів, що підтверджують авторство. Такі спеціальні відомості можуть розглядатися як докази при розгляді спорів про авторство або для доказу нелегального копіювання, чи володіння інформацією. [5]

На сьогодні в якості інструментів для розвитку цієї галузі широко використовуються методи теорії ймовірностей та математичної статистики, теорії швидких ортогональних перетворень, теорії апроксимації, теорії

кодування, теорії складності, теорії похибок, цифрової обробки сигналів та зображень тощо. [6]

Незважаючи на молодість комп'ютерної стеганофонії, основні її поняття та принципи не аналогічні стеганографії. Так в роботах [6-11] наведено базову систему означень та математичні моделі стеганографічних систем. Велика кількість вітчизняних та зарубіжних публікацій присвячена аналізу головної характеристики стегосистеми – її стійкості. [6]

Значний вклад в розвиток стеганографії у світі внесли I. Cox, Y. Li, N. Nikolaidis, R. Ohbuchi, I. Pitas, V. Solachidis, M. Voigt, Wojciech Mazurczyk, Krzysztof Szczypiorski,Zbigniew Kotulski та інших.[6]

В Україні й на пострадянському просторі - А.В. Аграновський, В.Г. Грибунін, В.К. Задірака, Є.А. Золотовкін, А.А. Кобозєва, Г.Ф. Конахович, О.О. Кузнецов, В.В. Лукічов, І.І. Маракова, О.А. Смірнов, В.О. Хорошко, М.Є. Шелест, Ю.Є. Яремчук, Кошкіна Н.В., Олексюк О.С та інші. [12][6]

Аналіз останніх досліджень і публікацій [1-2][7][13][24] показує, що у наукових публікаціях особливу увагу присвячено основним принципам та засобам забезпечення інформаційної безпеки, серед яких важливе місце посідає організація та здійснення прихованого обміну інформації на основі застосування методів комп'ютерної стеганографії.

Серед останніх досліджень і публікацій варто виділити дослідження, що стосуються аналітичного огляду великої кількості алгоритмів вбудовування, запропонованих за останні роки [2], класифікації стегосистем та методів вбудовування, формального математичного опису та структурної схеми стеганографічної системи захисту інформації на основі теорії секретних систем, проблем цифрової обробки сигналів, що виникають при вбудовуванні інформації, детального дослідження підвищення пропускної здатності стегоканалу, забезпечення стійкості та непомітності вбудовування [2].

Аналіз останніх досліджень і публікацій [1-2][13] показує, що найбільшу популярність в комп'ютерній стеганографії здобули стеганографічні методи, які використовують у ролі контейнера зображення.

Проведений аналіз показав, що однією з ключових проблем стеганографії є питання оптимального використання стегоконтейнера (підвищення пропускної здатності стегоканалу), оскільки потреба у передачі даних великого обсягу виникає частіше, ніж потреба передачі даних невеликого обсягу. [2]

Кожен з пропонованих раніше методів відрізняється своїми якісними характеристиками, проте пошук оптимального співвідношення місткості контейнера і його спотворення триває досі.

При роботі з даними великого обсягу важливим завданням є збільшення прискорення процесів шифрування, дешифрування інформації.

Тому завдання забезпечення захисту інформації, авторських прав, прав інтелектуальної власності або конфіденційності даних (які в більшості випадків мають цифрової формат) від несанкціонованого доступу є актуальними на сьогодні. Переваги подання та передачі даних у цифровому вигляді (легкість відновлення, висока потенційна завадостійкість, перспективи використання універсальних апаратних і програмних рішень) можуть бути перекреслені з легкістю, з якою можливі їх викрадення та модифікація [1].

Таким чином, актуальним науковим завданням, що має теоретичне і практичне значення, є розробка нових та удосконалення існуючих стеганографічних методів приховування інформації у зображення.

Об'єктом дослідження є процеси приховування інформації у зображення, а предметом - стеганографічні методи приховування графічної інформації з використанням матриці судоку.

Метою даної роботи є покращення якісних характеристик методу стеганографії з використанням матриці судоку.

В роботі використовуються методи наукової абстракції, аналізу і синтезу (при розкритті теоретичних положень та формулюванні категоріального

апарату), порівняння (для встановлення переваг та недоліків різних методів стеганографії), формалізації (для опису вимог до стегоконтейнера), емпіричні (для оцінки спотворень стегоконтейнера) та методи системного підходу.

В ході написання дисертації було проведено аналіз існуючих методів стеганографії та детально розглянуто стегосистеми.

Врахувавши сильні та слабкі сторони наявних методів було запропоновано модифікацію одного з методів стеганографії - з використанням матриці судоку.

Практична цінність отриманих в роботі результатів полягає в розробці програмного забезпечення, що є комплексним вирішення задачі приховування даних, спрощуючи використання стегосистеми, мінімізовуючи можливості випадкової втрати ключа або цілеспрямованого взлому.

Основні положення і результати роботи були представлені на 20-тій міжнародній конференції "Системний аналіз та інформаційні технології" ("System Analysis and Information Technologies") SAIT 2018 (21–24 травня 2018 року, Київ, Україна) та обговорювалися на X науковій конференції магістрантів та аспірантів «Прикладна математика та комп’ютинг» ПМК-2018 (21-23 березня 2018 року, Київ, Україна).

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ СТЕГАНОГРАФІЇ

1.1 Стеганографія. Основні поняття

Стеганографія - наука про методи захисту інформації шляхом приховування факту її існування в певному середовищі. Приховування факту існування таємного повідомлення завжди видавалося доцільним для його захисту, а наявність різних технічних, хімічних, фізичних і психологічних методів такого приховування забезпечувало можливість його реалізації. [14]

Перші згадки про стеганографію зустрічаються в праці давньогрецького історика Геродота «Історія», що відноситься до 440 року до н. е.. У трактаті йдеться про два методи стеганографії. У першому на поголену головою раба записувалося секретне повідомлення, а коли його волосся відростало, він вирушав до адресата, який знову голив його голову і зчитував повідомлення. Другий спосіб полягав у наступному: повідомлення наносилося на дерев'яну дощечку, а потім вона покривалася воском, і, тим самим, не викликала жодних підозр. Потім віск зіскоблюється, і повідомлення ставало видимим. [18]

Одним з найбільш поширених методів класичної стеганографії є використання невидимих чорнил. Текст, записаний такими чорнилом, проявляється лише за певних умов (нагрівання, спеціальне освітлення, хімічний проявник і т. д.). [19]

У Китаї листи писали на смужках шовку. Тому для приховування повідомлень, смужки з текстом листа, згорталися в кульки, покривалися воском і потім ковталися посильними.

У XV столітті чернець Трітеміус, що займався криптографією і стеганографією, описав багато різних методів прихованої передачі повідомлень. Пізніше, у 1499 році, ці записи були об'єднані в книгу «Steganographia».

Період XVII - XVIII століття відомий як ера «чорних кабінетів» - спеціальних державних органів з перехоплення, перлюстрації і дешифрування листування. У штат «чорних кабінетів», окрім криптографів і

дешифрувальників, входили й інші фахівці, в тому числі і хіміки. Наявність фахівців-хіміків було необхідно через активне використання невидимих чорнил. [20]

Стеганографічні методи активно використовувалися і в роки Громадянської війни в США. Так, в 1779 році два агента Семюель Вудхулл і Роберт Тоунсенд передавали інформацію Джорджу Вашингтону, використовуючи спеціальне чорнило.[20]

В основі багатьох підходів до вирішення завдань стеганографії лежить спільна із криптографією методична й інструментальна база, яка була закладена Шеноном при розробці загальної теорії секретного зв'язку. Це пов'язано з тим, що стеганографія й крипторафія розвивалися в рамках єдиної науки - тайнопису. Лише наприкінці XIX століття, після формулювання Кірхгофом базових законів криптографії, основний з яких полягав у тому, що стійкість криптографічного перетворення визначається таємністю ключа, криптографія відокремилася від стеганографії й стала розвиватися як самостійна наука. [14]

Сьогодні стеганографія являє собою сукупність методів і технічних рішень, що реалізують захист інформації, заснований на різних принципах. Зараз вона стала міждисциплінною наукою, що активно розвивається. Зокрема, починаючи приблизно з 2008 року нею стали цікавитися не тільки математики-криптографи, а й лінгвісти, філологи і навіть хіміки. [5] На даний момент в США зареєстровано 119 патентів з стеганографії, [15] в Росії - 63, [16] в Україні - 12 [17].

Однак в умовах стрімкого зростання інформаційно-телекомунікаційних технологій найактивніше розвиваються комп'ютерні методи стеганографії й способи їхнього застосування в кібернетичному просторі. [14]

Одним з найновіших напрямків стеганографії є лінгвістична стеганографія, що вивчає приховування конфіденційних повідомлень у тексті. Для цього використовується або звичайна надлишковість мови, або формати представлення тексту. Методи лінгвістичної стеганографії поділяють на:

методи довільного інтервалу (здійснюють вбудовування шляхом маніпуляції з пробільними символами), синтаксичні методи (працюють з пунктуацією), семантичні методи (до основи яких покладене залежне від приховуваних бітів даних маніпулювання словами).[1][3]

Як і будь-який новий напрямок, комп'ютерна стеганографія, незважаючи на велику кількість відкритих публікацій та щорічні конференції, довгий час не мала єдиної термінології.

До недавнього часу для опису моделі стеганографічної системи використовувалася запропонована 1983 Сіммонсом так звана "проблема ув'язнених". [21] Вона полягає в тому, що два індивідуума (Аліса і Боб) хочуть обмінюватися секретними повідомленнями без втручання охоронця (Віллі), контролюючого комунікаційний канал. При цьому є ряд припущень, які роблять цю проблему більш-менш розв'язуваною. Перше припущення полегшує вирішення проблеми і полягає в тому, що учасники інформаційного обміну можуть розділяти секретне повідомлення (наприклад, використовуючи кодову клавішу) перед укладанням. Інше припущення, навпаки, утрудняє вирішення проблеми, так як охоронець має право не тільки читати повідомлення, але і модифіковувати його. [21]

Пізніше, на конференції Information Hiding: First Information Workshop в 1996 році було запропоновано використовувати єдину термінологію та обговорено основні терміни [22].

Стеганографічна система або стегосистема (стеганосистема) – це сукупність засобів та методів, що використовуються для забезпечення прихованого каналу передачі даних.

В процесі побудови стегосистеми повинні враховуватися наступні положення:

- зловмисник має повне уявлення про стеганографічну систему і деталі її реалізації. Єдиною інформацією, яка залишається невідомою для потенційного зловмисника, є ключ, за допомогою якого тільки його

власник має можливість встановити факт наявності та зміст прихованого повідомлення;

- якщо зловмисник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому витягнути аналогічні повідомлення з інших даних до тих пір, поки ключ є невідомим;
- зловмисник не повинен мати технічні чи будь-які інші переваги у розпізнаванні або розкритті змісту таємних повідомлень. [20]

Узагальнену модель стегосистеми зображено на рис.1.1. [23]

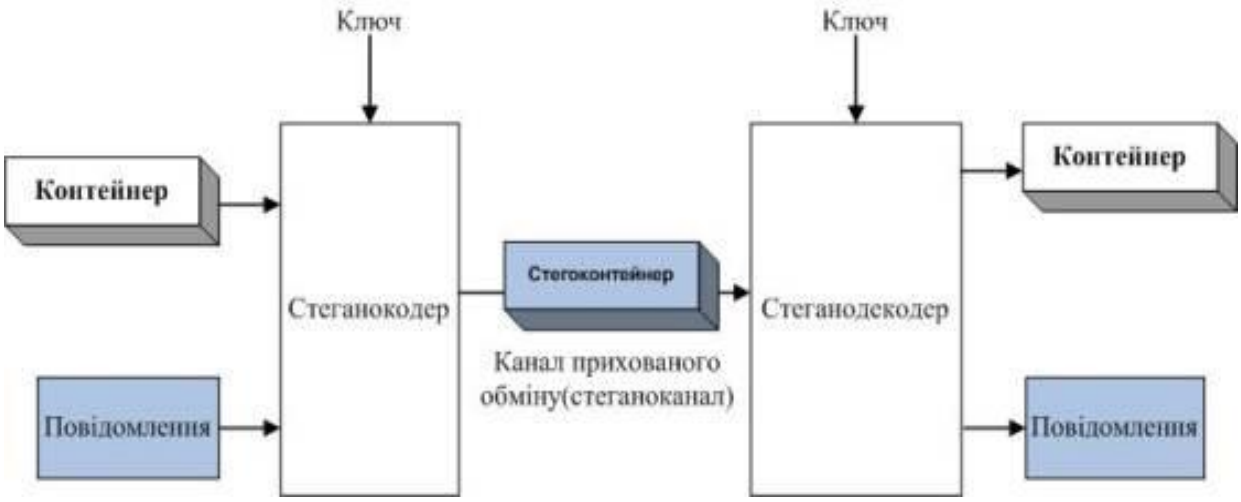


Рис.1.1. Узагальнена модель стегосистеми

В якості даних може використовуватися будь-яка інформація: текст, повідомлення, зображення і т. п.

У загальному випадку для позначення інформації, що приховується використовують термін "повідомлення". Повідомленням може бути як текстом чи зображенням, так і, наприклад, аудіофайлом.

Контейнер – будь-яка інформація, призначена для приховування таємних повідомлень. [1]

Порожній контейнер – контейнер без вбудованого повідомлення.

Заповнений контейнер або стегоконтейнер – контейнер, що містить вбудовану інформацію. [3]

Вбудоване (приховане або секретне) повідомлення – повідомлення, яке вбудоване в контейнер.

Стеганографічний канал або просто стегоканал – канал передачі контейнера.

Стегоключ або просто ключ – секретний ключ, необхідний для приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) у стегосистеми може бути один або кілька таких ключів. [20]

Аналогічно до криптографії, за типом стегоключа стегосистеми можна підрозділити на два типи:

- з секретним ключем;
- з відкритим ключем.

У стегосистеми з секретним ключем використовується один ключ, який повинен бути визначений або до початку обміну секретними повідомленнями, або переданий по захищеному каналу.

У стегосистеми з відкритим ключем для вбудовування і вилучення повідомлення використовуються різні ключі, які розрізняються таким чином, що за допомогою обчислень неможливо вивести один ключ з іншого. Тому один ключ (відкритий) може передаватися вільно по незахищеному каналу зв'язку. Крім того, дана схема добре працює і при взаємній недовірі відправника і одержувача. [20]

У процесі передачі відео, зображення або будь-яка інша інформація, що використовується у якості контейнера, може зазнавати різних трансформацій (у тому числі з використанням алгоритмів із втратою даних): зміна об’єму, перетворення у інший формат тощо. Тому для збереження цілісності вбудованого повідомлення може знадобитися використання коду з виправленням помилок (завадостійке кодування). [4]

Для того, щоб стегосистема була надійною і якісною, при її проектуванні необхідне виконання ряду вимог: [20]

- Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення у візуально незначущі області сигналу. Однак, ці ж області використовують і алгоритми стиснення. Тому, якщо зображення буде надалі піддаватися стисненню, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися в візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів.
- Стегосистема цифрового водяного знаку (ЦВЗ) повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить. У деяких додатках таке виявлення може призвести до серйозних наслідків.
- Повинна забезпечуватися необхідна пропускна здатність.
- Стегосистеми повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВЗ, тобто складний стеганокодер і простий стеганодекодер. [4]

За рівнем забезпечення таємності стегосистеми поділяються на теоретично стійкі, практично стійкі і нестійкі системи [11].

Теоретично стійка (абсолютно надійна) стегосистема здійснює приховування інформації лише в тих фрагментах контейнера, значення елементів яких не перевищують рівень шумів або помилок квантування, і при цьому теоретично доведено, що неможливо створити стеганоаналітичний метод виявлення прихованої інформації.

Практично стійка стегосистема проводить таку модифікацію фрагментів контейнера, зміни яких можуть бути виявлені, але відомо, що на даний момент необхідні стеганоаналітичні методи у зловмисника відсутні або поки що не розроблені.

Нестійка стегосистема приховує інформацію таким чином, що існуючі стеганоаналітичні засоби дозволяють її виявити. У цьому випадку стеганографічний аналіз допомагає знайти уразливі місця стеганографічного перетворення і провести його удосконалення таким чином, щоб усі зміни, внесені до контейнеру, знову виявилися б в області теоретичної або практичної нерозрізненості. [3]

1.2 Критерії оцінювання стегосистем

Для того, щоб методи стеганографії можна було порівнювати було виділено критерії оцінки стегосистем.

На рис.1.2 наведено схему класифікації критеріїв оцінки стегосистем.

1.2.1 Кількісні показники

Для порівняльного оцінювання ефективності стеганографічних засобів використовуються існуючі кількісні показники, які оперують із зображеннями на рівні пікселів, хоча після належної адаптації вони можуть бути застосовні й до інших способів опису зображення, а також до аудіо даних [3].

Найбільш популярним показником при аналізі рівня спотворень, які вносяться в контейнер під час приховування в ньому інформації, є взяте з радіотехніки співвідношення «сигнал/шум» (SNR - Signal Noise Ratio). Воно є безрозмірною величиною, рівною відношенню корисного сигналу до шуму. Чим більше це співвідношення, тим менше шум спотворює зображення. [4]

Обчислюється за формулою:

$$SNR = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2},$$

де $C_{x, y}$ – значення пікселя порожнього контейнера з координатами (x,y),

$S_{x, y}$ – відповідне значення пікселя заповненого контейнера,

rows (C) – кількість рядків у масиві C,

cols (C) – кількість стовпців у масиві C.

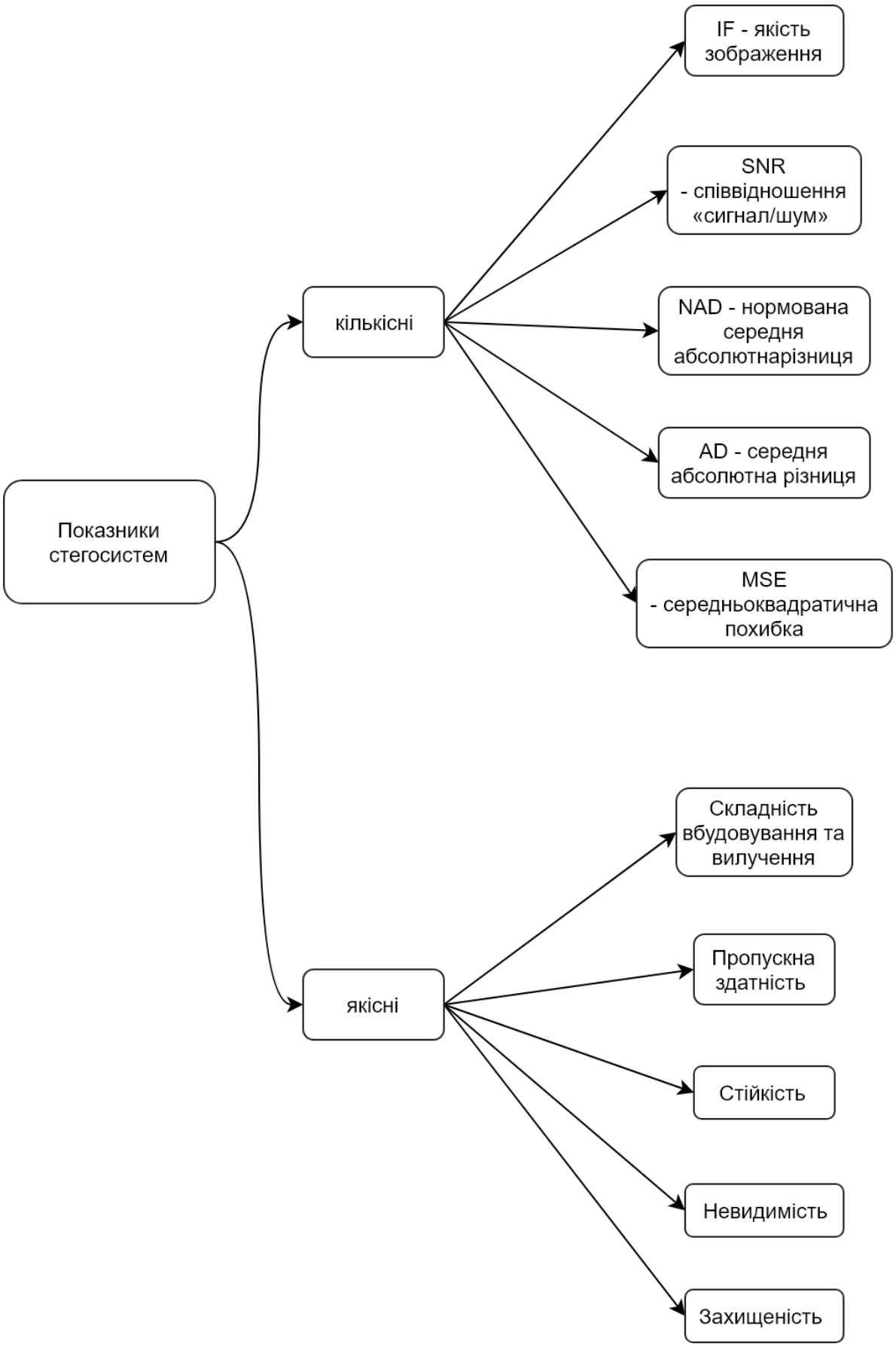


Рис.1.2. Класифікація критеріїв оцінки стегосистем

NAD (Normalized Average Absolute Difference) - нормована середня абсолютна різниця. Показує ступінь відмінності між вихідним контейнером і контейнером з вбудованим секретним файлом. [4] Розраховується в такий спосіб:

$$NAD = \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right|}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} \right|}.$$

IF (Image Fidelity) - якість зображення. Є однією з основних характеристик, що оцінюються у стеганографічних методах, які працюють із зображеннями. Тому що візуальна атака заснована на здатності зорової системи людини аналізувати зорові образи й виявляти істотні розходження в зображеннях. [1] Вона характеризує ступінь відповідності порожнього контейнера до заповненого. Обчислюється в за формулою:

$$IF = 1 - \frac{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2}{\sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y})^2}.$$

MSE (Mean Square Error) - середньоквадратична похибка. Є середньоквадратичним відхиленням вибіркового розподілу статистичних даних. Тобто, її можна використовувати для оцінки точності вибіркового середнього значення. [4] Розраховується за формулою:

$$MSE = \frac{1}{X \cdot Y} \sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} (C_{x,y} - S_{x,y})^2.$$

AD (Absolute Difference) - середня абсолютна різниця. Визначає середнє значення модулю різниці між пікселями порожнього і заповненого контейнеру. Велике значення AD вказує на низьку якість зображення. Обчислюється за формулою [4]:

$$AD = \frac{1}{X \cdot Y} \sum_{x=1}^{row(C)} \sum_{y=1}^{cols(C)} \left| C_{x,y} - S_{x,y} \right| .$$

1.2.2 Якісні показники

До найважливіших якісних характеристик стеганографічних систем, утворених з використанням різних методів, належать:

Пропускна здатність (Capacity) – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру. Стегосистема повинна забезпечувати необхідну пропускну здатність [4].

Стійкість (Robustness) – це здатність вилучити приховану інформацію після загальних операцій з обробки зображень: лінійні і нелінійні фільтри (розмитість, підвищення різкості, медіанна фільтрація), стиснення з втратами, регулювання контрастності, перефарбування, передискретизації, масштабування, обертання, додавання шуму, обрізки, друку/копіювання/сканування, перестановки пікселів у вузькій околиці [1][4], квантування кольорів тощо. Передбачається, що поняття стійкості не включає атаки на методи вбудовування, які ґрунтуються на знанні алгоритму приховування або вилучення. Стійкість означає, стійкість до «сліпих», нецільових модифікацій, або загальних операцій із зображеннями.

Невидимість (Invisibility, Perceptual transparency) – це показник, що характеризує неспроможність зорової системи людини (ЗСЛ) помітити наявність секретного повідомлення без застосування для цього спеціальних засобів. Таємні дані вважаються непомітними, за умови, якщо середньостатистичній людині не вдається відрізнити незаповнений контейнер від заповненого.

Оцінку даного показника можна здійснювати за загальноприйнятою схемою експерименту (так званий сліпий тест), яка часто використовується в психо-візуальних експериментах: суб’єктам пропонується в довільному

порядку велика кількість заповнених і пустих контейнерів, їм потрібно обрати, які саме носії містять секретну інформацію [3-4].

Поняття невидимості може бути визначене й іншим способом та бути пов’язаним із статистичною моделлю джерела зображення. В такому випадку вважається, що прихована інформація є невидимою, якщо заповнене зображення-контейнер узгоджується з моделлю джерела, звідки було взяте вихідне зображення, і може бути розраховане об’єктивним шляхом, наприклад, за допомогою показника IF.

Захищеність (Security) – вбудовані дані не можуть бути видалені за допомогою цілеспрямованих атак, заснованих на відомому алгоритмі вилучення та вбудовування, і знанні принаймні одного носія з прихованим повідомленням. Поняття захищеності також включає в себе процедурні атаки, такі як атаки на основі знання про часткову модифікацію контейнера через наявність вбудовування [1-4].

Складність вбудовування/вилучення – кількість стандартних операцій, що необхідно виконати для вбудовування і виявлення секретного повідомлення. (Як було зазначено, стегосистеми повинні мати прийнятну обчислювальну складність реалізації).

Вищевказані вимоги взаємно конкуруючі і не можуть бути оптимальними одночасно. Якщо необхідно приховати велике повідомлення всередині зображення, то неможливо вимагати дуже великої невидимості і високої стійкості. Завжди необхідний певний компроміс, який буде задовільним в певній ситуації. З іншого боку, якщо потребується стійкість до великих спотворень, то повідомлення, що має бути надійно приховане, не може бути занадто довгим. [3-4]

Цю закономірність відображено на рис.1.3. [4]

Рис. 1.3. Співвідношення між якісними показниками стегосистем

1.3 Види атак на стегосистеми

Стегосистема вважається зламаною, якщо зловмисникові вдалося, принаймні, довести існування прихованого повідомлення в перехопленому контейнері. Передбачається, що він здатний проводити будь-які види атак. Якщо йому не вдається підтвердити гіпотезу про те, що в контейнері приховано секретне повідомлення, то стеганографічна система вважається стійкою. [3]

У більшості випадків виділяють декілька етапів зламу стеганографічної системи:

- виявлення факту присутності прихованої інформації;
- видобування прихованого повідомлення;
- видозміна (модифікація) прихованої інформації;
- заборона на здійснення будь-якого пересилання інформації, у тому числі і прихованої [1][4].

Перші два етапи відносяться до пасивних атак на стегосистему, а останні – до активних (або зловмисних) атак. Виділяють такі види атак на стегосистеми (за аналогією з криптоаналізом) [11]:

- атака на основі відомого заповненого контейнера.

У цьому випадку у розпорядженні зловмисника знаходиться один або декілька заповнених контейнерів (в останньому випадку передбачається, що вбудовування прихованої інформації здійснювалося тим самим способом). [1] Завдання зловмисника може полягати у виявленні факту наявності стегоканалу (основне завдання), а також у видобуванні даних чи визначенні ключа. Знаючи ключ, він матиме можливість аналізу інших стегоповідомлень;

- атака на основі відомого вбудованого повідомлення.

Цей тип атак більш характерний для систем захисту інтелектуальної власності, коли в якості ЦВЗ, наприклад, використовується відомий логотип фірми. Завданням аналізу є одержання ключа. Якщо відповідний прихованому повідомленню заповнений контейнер невідомий, то завдання дуже важко розв’язати; [11]

- атака на основі обраного прихованого повідомлення.

У цьому випадку зловмисник може пропонувати для передачі свої повідомлення й аналізувати отримувані при цьому результуючі контейнери;

- адаптивна атака на основі обраного прихованого повідомлення.

Ця атака є окремим випадком попередньої. При цьому зловмисник має можливість обирати повідомлення для нав’язування їх адаптивно, в залежності від результатів аналізу попередніх контейнерів-результатів. [6]

- атака на основі обраного заповненого контейнера.

Такий тип атаки є більше характерним для систем ЦВЗ. Стеганоаналітик має детектор заповнених контейнерів у вигляді “чорного ящика” і декілька таких контейнерів. Аналізуючи продетектовані приховані повідомлення, зловмисник намагається розкрити ключ. Крім того, у нього може існувати можливість застосувати ще три атаки, які не мають прямих аналогій у криптоаналізі; [3]

- атака на основі відомого порожнього контейнера.

Якщо останній є відомим зловмиснику, то шляхом порівняння його з підозрюваним на присутність прихованих даних контейнером, той завжди може

встановити факт наявності стегоканалу. Незважаючи на тривіальність цього випадку, у ряді робіт приводиться його інформаційно-теоретичне обґрунтування. Набагато цікавішим виглядає сценарій, коли контейнер відомий приблизно, з деякою похибкою (як це може мати місце при додаванні до нього шуму). У цьому випадку існує можливість побудови стійкої стегосистеми [1];

- атака на основі обраного порожнього контейнера.

У цьому випадку зловмисник може змусити користуватися запропонованим ним контейнером. Останній, наприклад, може мати більші однорідні області (однотонні зображення), і тоді буде важко забезпечити таємність вбудовування;

- атака на основі відомої математичної моделі контейнера або його частини.

При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі. Наприклад, можна припустити, що біти всередині певної частини зображення є корельованими. Тоді відсутність такої кореляції може служити сигналом про наявне приховане повідомлення. Завдання того, хто вбудовує повідомлення, полягає у тому, щоб не порушити статистики контейнера. Відправник і той, хто атакує, можуть мати у своєму розпорядженні різні моделі сигналів, тоді в інформаційно-приховуючому протиборстві, переможе той, хто має ефективнішу модель. [1][3]

Основна мета атаки на стеганографічну систему аналогічна атакам на криптосистему з тією лише різницею, що різко зростає значимість активних (зловмисних) атак. [1] Будь-який контейнер може бути замінений з метою видалення або руйнування прихованого повідомлення, незалежно від того, існує воно в контейнері чи ні. Виявлення існування прихованих даних зберігає час на етапі їхнього видалення, тому що буде потрібно обробляти тільки ті контейнери, які містять приховану інформацію. Навіть за найкращих умов для атаки, задача видобування прихованого повідомлення з контейнера може виявитися дуже складною. Однозначно стверджувати про факт існування

прихованої інформації можна лише після її виділення в явному вигляді. Іноді метою стеганографічного аналізу є не алгоритм взагалі, а пошук, наприклад, конкретного стегоключа. [3]

Кількісне оцінювання стійкості стеганографічної системи захисту до зовнішніх впливів являє собою досить складну задачу, яка зазвичай на практиці реалізується методами системного аналізу, математичного моделювання або експериментального дослідження. [6]

На рис.1.4 зображено підсумовуючу модель аналізу загроз та стійкості стегосистем.

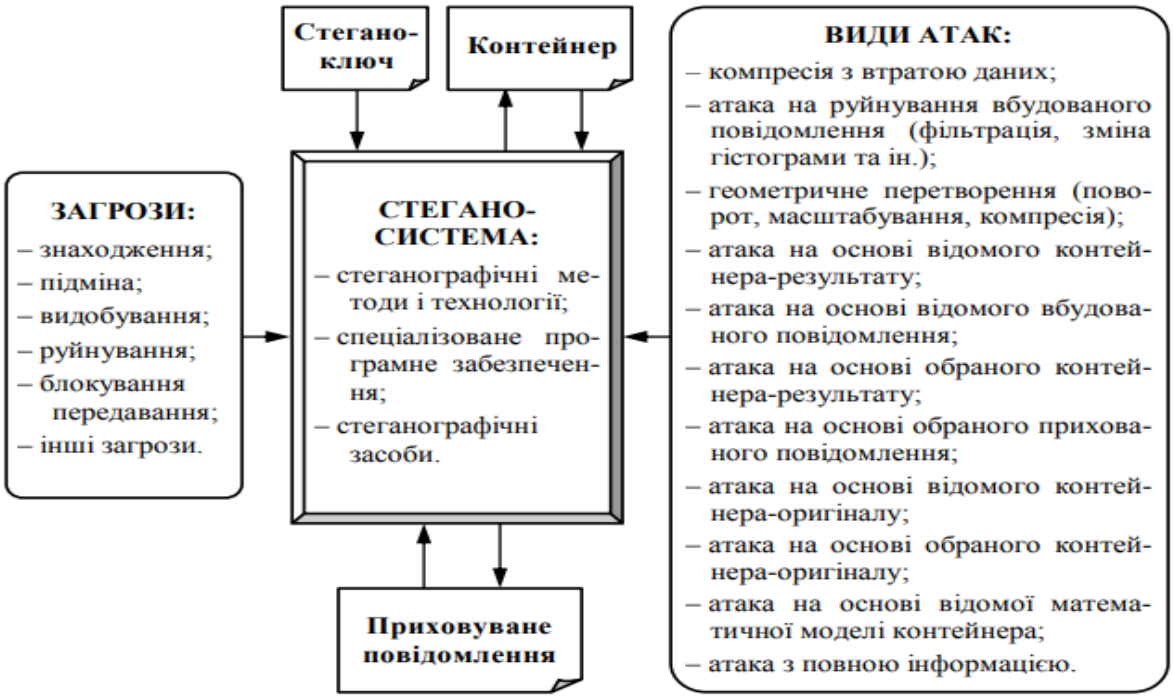


Рис.1.4. Модель аналізу загроз та стійкості стегосистем

1.4 Завдання та застосування стеганографії

Класичною ціллю стеганографії є прихована передача даних (ППД). Вона полягає в передачі інформації таким чином, щоб зловмисник не здогадався про сам факт існування прихованого повідомлення. Окрім цього, її цілями також є: цифрові підписи (ЦП) (Digital Fingerprint), стеганографічні або цифрові водяні знаки (СВЗ або ЦВЗ) (Stego Watermarking). [5]

Три перераховані цілі не можна об’єднувати і змішувати, так як методи для їх досягнення (завдання і проблеми, що виникають в ході реалізації) дуже

відрізняються. Прихована передача даних зовсім не те саме, що ЦП і ЦВЗ. Метою ППД є сама передача даних, а метою ЦП і ЦВЗ - захист контейнера, що їх містить. [5] Факт наявності ЦП або ЦВЗ може не бути таємницею (як у випадку водяних знаків на грошових купюрах), а в разі прихованої передачі даних втрата секретності наявності інформації означає провал операції.

Цифрові підписи передбачають наявність різних стеганографічних міток для кожної копії контейнера.

Якщо за допомогою будь-якого алгоритму зловмисник зможе витягнути ЦП з контейнера, то ідентифікувати його неможливо, але до тих пір, поки він не навчиться підробляти ЦП. Це означає, що незаконне поширення контейнера з ЦП можна виявити.

Стеганографічні водяні знаки, на відміну від ЦП, передбачають наявність однакових міток для кожної копії контейнера. [1]

Розглянемо детальніше задачі, для вирішення яких можна застосувати стеганографію.

1. Непомітна передача інформації. На відміну від криптографічних методів (які лише шифрують дані) стеганографія може застосовуватися як метод передачі інформації, не викликаючи підозр. Це завдання є «класичним практичним застосуванням» стеганографії.

2. Приховане зберігання інформації. Дана задача схожа на попередню, але в цьому випадку стеганографія використовується не для передачі, а для зберігання будь-якої інформації, виявлення самого факту наявності якої (навіть в зашифрованому вигляді) користувачу недопустимо. Очевидно, що ця задача реалізовується лише на носіях даних, а не в каналах зв’язку.

3. Недекларованe зберігання інформації. Велика кількість інформаційних ресурсів дозволяють зберігати дані тільки певного виду.

Наприклад портал YouTube дозволяє зберігати тільки відеоінформацію у форматах MOV, MPEG4, AVI, WMV, MPEG-PS, FLV, 3GPP, WebM. Однак використовуючи стеганографію, можна зберігати дані і в інших форматах.

Наприклад, сайт hid.im дозволяє користувачам приховувати файли .torrent всередині зображень PNG. [5]

4. Захист виключного права. Застосовується при продажі інформаційних ресурсів. Це можуть бути книги, фільми, музика, програмне забезпечення (ПЗ) і т.д.. Кожна копія повинна містити ЦП для ідентифікації особи або СВЗ для перевірки ліцензії копії. [3]

Наприклад, у 2007-2011рр. компанія Амазон використовувуала ЦП для збереження інформації про покупку музики [5].

5. Захист авторського права. СВЗ можна використовувати для підтвердження авторського права.

Наприклад, під час запису на відеокамеру можна в кожен кадр вбудовувати інформацію про час зйомки, модель відеокамери і т.д.. Отже, файл буде мати прив’язку до відеокамери, а оператор зможе довести авторство.

6. Запобігання витоку інформації (Data Leak Prevention, DLP). СВЗ можна застосовувати для запобігання витоку інформації. При створенні документа, що містить конфіденційну інформацію, вбудовується певна мітка. При цьому вонане змінюється, незалежно від кількості копій чи версій документа. Для того, щоб витягти мітку потрібно мати стегоключ, який зберігається в таємниці. DLP-система, перед тим як видати документ, перевіряє наявність СВЗ і якщо знак присутній, вона не дозволяє відправляти документ. [3]

7. Прихована передача керуючого сигналу. Припустимо, що одержувачем є певна система (наприклад супутник) а відправником є оператор. В даному випадку стеганографія може бути застосовна для доставки керуючого сигналу системі. Якщо система може знаходиться в різних станах і потрібно, щоб зловмисник не зміг дізнатись про те, що вона перейшла в інший стан, можна скористатися стеганографією. [5] Використання тільки криптографії, може дати зловмиснику інформацію про те, що щось змінилося і спровокувати його на небажані дії.

8. Підтвердження достовірності переданої інформації. Секретне повідомлення в даному випадку містить інформацію (контрольна сума або хеш-функція), що підтверджує коректність даних, що передаються контейнером.

Наприклад, якщо мова йде про фотографії, то захистом автентичності є доказ того, що дана фотографія справжня. Ми ніби захищаємося від самого відправника (в даному випадку фотографа). У разі підтвердження достовірності необхідно організувати захист від третьої сторони (man in the middle), яка має можливість підробити дані між відправником і отримувачем. [5] Дана проблема має багато класичних рішень, в тому числі криптографічних. Використання стеганографії є ще одним способом її вирішення.

9. Funkspiel. Секретне повідомлення в даному випадку містить дані, що вказують на те, чи варто сприймати інформацію контейнера всерйоз. Це також може бути хеш-функція або наперед встановлена послідовність біт. Якщо секретне повідомлення не пройшло перевірку, одержувачам потрібно ігнорувати контейнер, незалежно від його вмісту. В даному випадку стеганографія може бути використана для дезінформації зловмисника.

Наприклад, контейнер може бути криптографічним повідомленням. У цьому випадку відправник, бажаючи ввести в оману зловмисника, шифрує дані відомим для зловмисника криптографічним ключем, а стегоповідомлення використовується з метою, щоб одержувач не сприйняв помилковий контейнер всерйоз. [5] На практиці доцільно поєднувати funkspiel та підтвердження достовірності переданої інформації.

10. Забезпечення цілісності інформації. Якщо є необхідність мати документи в такому вигляді, щоб неможливо було одну інформацію відокремити від іншої, можна використовувати СВЗ.

Приклади використання: медичні знімки з вбудованою інформацією про пацієнтів, скріншоти гри WoW з вбудованою інформацією про користувача, датою створення, адресою сервера. [5]

1.5 Висновки до розділу

У першому розділі були отримані результати:

- Наведено основні поняття стеганографії (стегосистема, контейнер, ключ, секретне повідомлення, стегоканал).
- Історію її розвитку стеганографії від найдавніших часів, до сьогодення.
- Обґрунтовано актуальність використання стеганографії для вирішення сучасних задач.
- Розглянуто класифікацію показників, які дають кількісні та якісні оцінки для порівняння стеганографічних систем. До кількісних оцінок належать: SNR, IF, NAD, AD, MSE. До найважливіших якісних характеристик належать: пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення.
- Розглянуто різні види атак, описано модель аналізу загроз та стійкості стегосистем.
- Наведено завдання (ППД, ЦП, ЦВЗ), та сфери застосування стеганографії з реальними прикладами. Серед задач, для вирішення яких підходить стеганографія було розглянуто такі: непомітна передача інформації, приховане зберігання інформації, недекларованe зберігання інформації, захист виключного права, захист авторського права, запобігання витоку інформації, прихована передача керуючого сигналу, підтвердження достовірності переданої інформації, funkspiel, забезпечення цілісності інформації.

2 ПОРІВНЯННЯ ІСНУЮЧИХ РІШЕНЬ СТЕГАНОГРАФІЇ ЗОБРАЖЕНЬ ТА ОБҐРУНТУВАННЯ ТЕМИ МАГІСТЕРСЬКОЇ ДИСЕРТАЦІЇ

Більшість сучасних досліджень присвячено використанню в якості стегоконтейнерів саме цифрових зображень. Це обумовлено наступними причинами:

- існуванням практичної необхідності захисту цифрових фотографій, відео від протизаконного поширення;
- відносно великим обсягом цифрового представлення зображень, що дозволяє вбудовувати ЦВЗ великого обсягу або ж підвищувати стійкість такого вбудовування; [4]
- заздалегідь відомим або фіксованим розміром стегоконтейнера, відсутністю обмежень, що накладаються вимогами приховування у реальному часі;
- наявністю в більшості реальних зображень областей, що мають шумову структуру і тому добре підходять для вбудовування інформації;
- слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, вмісту в ньому шуму, зміни поблизу контурів;
- активним розвитком методів цифрової обробки зображень. [1][3]

Але остання причина викликає й значні труднощі в забезпеченні стійкості ЦВЗ: з вдосконаленням методів компресії, менше залишається можливостей для вбудовування секретних повідомлень. Розвиток теорії й практики алгоритмів компресії зображень призвів до зміни уявлень про техніку вбудовування ЦВЗ. [3] Якщо спочатку пропонувалося вбудовувати інформацію в незначущі біти для зменшення візуальної помітності (метод найменш значущого біта - НЗБ), то сучасний підхід, навпаки, полягає у вбудовуванні ЦВЗ

у найбільш істотні області зображень, руйнування яких може призвести до повної деградації самого зображення. [1]

Отже, при розробці сучасних методів стеганографії цілком зрозумілою є необхідність врахування не лише властивостей ЗСЛ, але й алгоритмів компресії цифрових зображень.

2.1. Властивості зорової системи людини

Властивості ЗСЛ розділяють на дві категорії: низькорівневі (або фізіологічні) та високорівневі (або психофізіологічні) [3-4].

Серед низькорівневих властивостей виділяють три найважливіших, які впливають на помітність шуму в зображенні:

- чутливість до зміни яскравості (контрастності) зображення;
- частотна чутливість;
- ефект маскування. [4]

На рис.2.1 зображена залежність мінімального контрасту ΔI/I від яскравості.

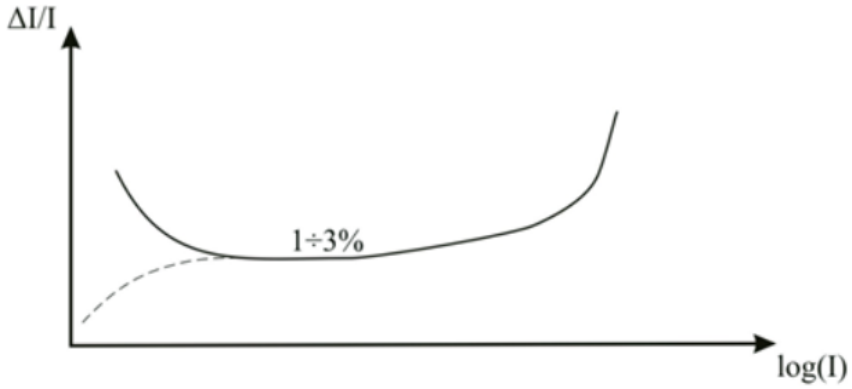


Рис. 2.1. Чутливість до зміни контрасту і поріг непомітності ΔI

Як видно, для середнього діапазону зміни яскравості контраст приблизно постійний, в той час, як для малих і великих значень яскравості значення порога непомітності (ΔI) зростає. Встановлено, що $\Delta I \approx (0.01 \div 0.03) \cdot I$ для середніх значень яскравості. [1]

Окрім цього, у [4] зазначено, що результати новітніх досліджень суперечать «класичній» теорії і показують, що при малих значеннях яскравості

поріг непомітності зменшується, тобто ЗСЛ більш чутлива до шуму в цьому діапазоні.

Частотна чутливість ЗСЛ проявляється у тому, що людина більш сприйнятлива до низькочастотного (НЧ), ніж до високочастотного (ВЧ) шуму. Це пов'язано з нерівномірністю амплітудно-частотної характеристики ЗСЛ. [3]

Елементи ЗСЛ поділяють сигнал, що надходить, на окремі складові, кожна з яких збуджує нервові закінчення очей через ряд підканалів. Складові, що виділяються оком, мають різні просторові і частотні характеристики, а також різну просторову орієнтацію (горизонтальну, вертикальну та діагональну)[4].

У разі одночасного впливу на око двох складових зі схожими характеристиками збуджуються одні й ті ж підканали. Це призводить до ефекту маскування, який полягає у збільшенні порога виявлення зорового сигналу в присутності іншого сигналу, що має аналогічні характеристики. Тому, адитивний шум є набагато помітнішим на НЧ (однотонних) ділянках зображення в порівнянні з ВЧ ділянками. Те, що спостерігається в останньому випадку називається ефектом маскування. Найбільш сильно цей ефект проявляється тоді, коли обидва сигнали мають однакову просторову орієнтацію і місце розташування [4].

Частотна чутливість тісно пов'язана з яскравістю. Відомо також і вираз для визначення порогу маскування на основі відомої яскравісної чутливості, що дозволяє знайти метрику спотворення зображення, яка би враховувала властивості ЗСЛ. Для цього випадку розроблено детальні математичні моделі квантування коефіцієнтів ДКП, оскільки саме воно застосовується у стандарті JPEG.

Високорівневі властивості ЗСЛ відрізняються від низькорівневих тим, що проявляються «вторинно» – обробивши первинну інформацію від ЗСЛ, мозок видає команди на «підстроювання» зорової системи під зображення.

Перелічимо основні з цих властивостей: [1-4]

- чутливість до контрасту. Полягає в тому, що висококонтрастні ділянки зображення і перепади яскравості звертають на себе більше уваги;
- чутливість до розміру. Проявляється в тому, що великі ділянки зображення є більш помітними у порівнянні з меншими за розміром, причому існує поріг насиченості, при досягненні якого, подальше збільшення розміру не є важливим;
- чутливість до форми. Спостереження показують, що довгі і тонкі об'єкти привертають більше уваги, ніж закруглені і однорідні;
- чутливість до кольорів. Полягає в тому, що деякі кольори є більш помітними, ніж інші (рис.2.2). [1] Як показує практика, даний ефект посилюється, те, що на задньому плані відрізняється від кольорів фігур на ньому або елементів переднього плану;
- чутливість до місця розміщення. чутливість до зовнішніх подразників. Полягає в тому, що рух очей людини залежить від обстановки, отриманих нею перед переглядом або під час інструкцій, додаткової інформації і тд.;
- Полягає в тому, що люди схильні більше вдивлятися у центр зображення; також уважніше розглядаються предмети переднього плану, ніж заднього. [4]

Дотримуючись рекомендацій по роботі ЗСЛ, можна запобігти виявленню прихованих даних методом візуальної атаки. Бо саме вона заснована на здатності ЗСЛ аналізувати зорові образи й виявляти всякі розбіжності в зображеннях. [4]

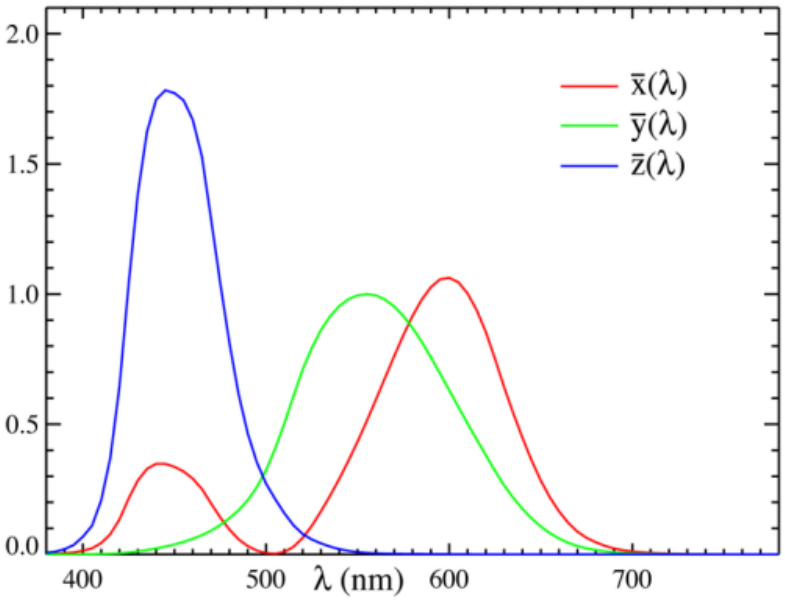


Рис. 2.2. Функції колірної відповідності Стандартного колориметричного спостерігача

2.2. Аналіз цифрових зображень як потенційних стегоконтейнерів

В сучасному процесі поліграфічного виробництва всі ілюстрації й елементи оформлення представлені цифровими зображеннями різних типів. Цифрові зображення за способом дискретизації оригіналу поділяються на растрові, векторні та змішаного типу. Класифікацію форматів цифрових зображень наведено на рис.2.3.

До растрових зображень відносяться двомірні масиви даних (матриці пікселів), кожен елемент яких представляє ділянку оригіналу з усередненим колірним показником [4].

Растрові зображення отримують двома способами. Перший – сканування растрового зображення – проводиться за допомогою особливого пристрою – сканера, в якому кожен оптичний елемент ПЗЗ-лінійки (або ПЗЗ-матриці) зчитує яскравості і колірні характеристики оригіналу. Ці характеристики перетворюються в двійковий код кольору і посилаються в осередку двомірного масиву даних (матриці пікселів). Другий спосіб отримання растрового зображення – проектування оригіналу на ПЗЗ-матрицю через систему лінз

(об'єктив). Цей спосіб растрового аналого-цифрового перетворення характерний для цифрових фотоапаратів та відеокамер.

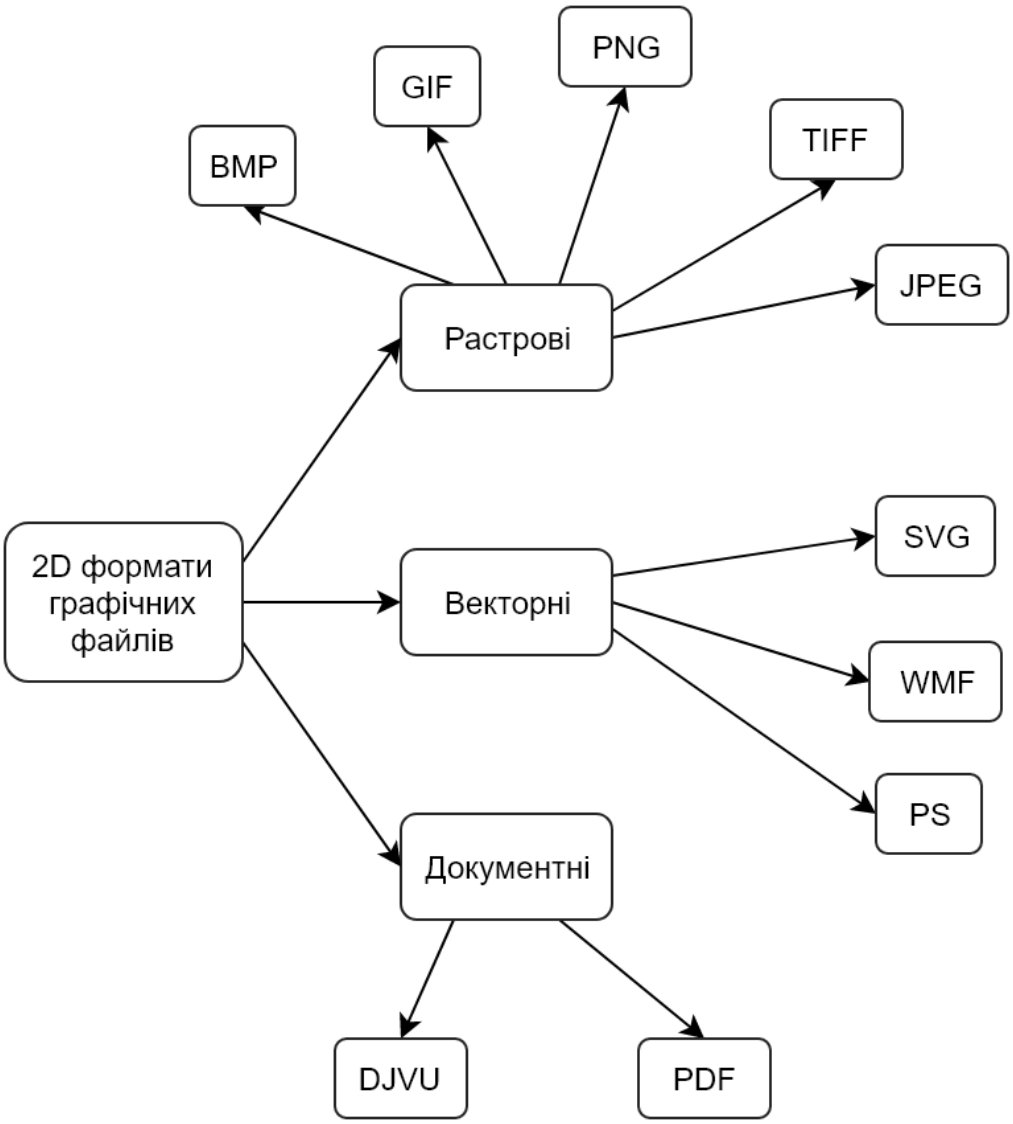


Рис. 2.3. Класифікація форматів графічних файлів

Основними характеристиками растрового зображення є розмір та глибина кольору.

Глибина кольору – це характеристика, яка визначає якість відтворення кольору, кількість відтінків, які можуть відображати елементи матриці пікселів. Кожен елемент масиву даних (матриці) являє собою число в двійковій системі числення. Його розмірність визначається в бітах. Глибина кольору – це кількість біт на піксель зображення. За допомогою одного байта (8 біт) можна задати 256 кольорів (як правило чорно-білих). Колір пікселя задається як

поєднання трьох кольорів (червоного, зеленого, блакитного) у різних відношеннях (рис.2.4), схема RGB.

Розмір зображення в пікселях – це кількість рядків і стовпців матриці, які використовуються для збереження зображення. Його можна довільно змінювати, змінюючи фізичний розмір зображення при друку, при цьому розмір матриці пікселів буде залишатися сталим.

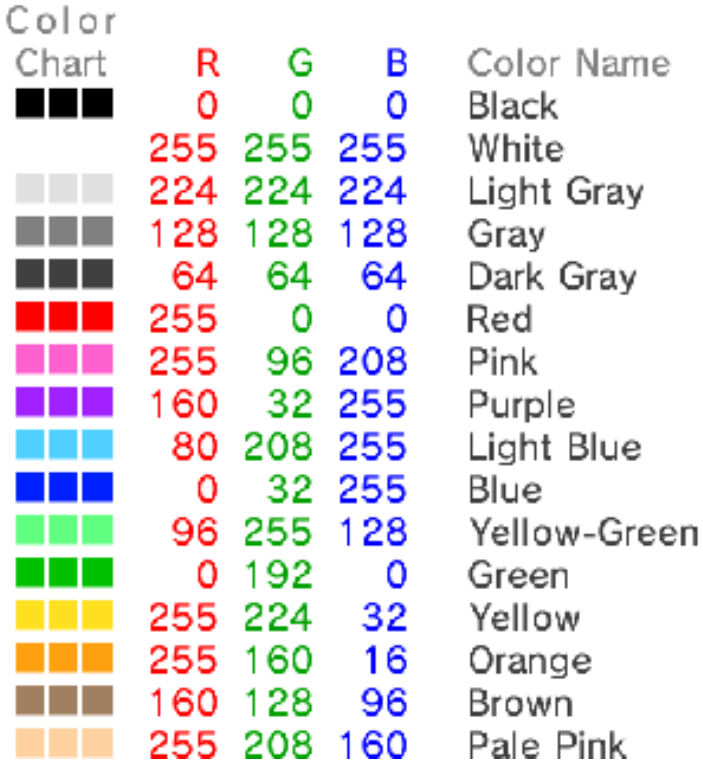


Рис. 2.4. Приклади представлення кольорів пікселя через три кольорових компоненти (схема RGB)

При аналого-цифровому перетворенні завжди відбувається втрата деякої кількості інформації, оскільки дискретизація завжди проводиться шляхом усереднення та узагальнення потоку вихідної аналогової інформації. Звідси основний недолік растрових цифрових зображень – неможливість їх масштабування без втрати якості.

Основна сфера застосування растрових зображень – це фотографічні ілюстрації. Растрові зображення використовуються у всіх випадках, коли необхідно відтворити аналоговий оригінал, будь то фотографія, малюнок, складний елемент оформлення, який нераціонально переводити в вектори.

Зовсім іншим видом цифрових зображень є векторні зображення. Найменшими елементами векторного зображення є вектор і крива Безьє. Основним керуючим елементом кривої Безьє є вузол, що також називається контрольною точкою або контрольною вершиною. Ступінь кривизни лінії визначаються координатами вузла і двох керуючих точок [4]. Контур зображення в цифровому вигляді являє собою масив даних, що містить координати контрольних та керуючих точок, а також характеристики кривої в цілому – її товщину, колір, напрямок, а якщо крива замкнута – то і колір і тип заливки.

Векторні зображення отримують двома способами – шляхом ручного трасування оригіналу і шляхом автоматичного трасування. Основна перевага векторного зображення – це можливість масштабування без втрати якості. Ще одним плюсом векторних зображень є порівняно невеликий розмір файлів, що їх містять. Це робить зручною передачу векторних зображень по електронних каналах зв'язку.

Головний недолік векторних зображень – це те, що вони майже завжди відтворюють оригінал в спрощеному вигляді (рис.2.5). Деякі деталі оригіналу буває неможливо відтворити у векторному зображенні. Часто векторні зображення не є повноцінними ілюстраціями.

Рис. 2.5. Приклад растрового та векторного зображень

Цифрові зображення змішаного типу являють собою масиви даних, що містять інформацію як у вигляді матриці пікселів, так і у вигляді опису векторів, кривих Безьє, примітивів і текстових блоків [4].

В основі вертикальної структури векторно-растрових зображень лежить поняття шару. Шар – це область даних, що містить інформацію про окремий елемент вертикальної структури зображення.

Векторно-растрові зображення отримують з вихідних векторних і растрових елементів шляхом зведення за допомогою графічних редакторів. Також умовно до зображень змішаного типу слід віднести результати роботи програм комп'ютерної верстки, в яких якості основного векторного елемента виступають текстові блоки. [3-4]

Зображення змішаного типу поєднують в собі переваги та недоліки тих типів зображень, які присутні в них у вигляді елементів або шарів.

Основною перевагою зображень змішаного типу є можливість вільного редагування кожного шару окремо, а основним недоліком – великий обсяг масиву даних і, відповідно, кінцевого файлу. [4]

Отже, не зважаючи на деякі недоліки растрових зображень, вони є найпоширенішими у використанні – растрова графіка використовується майже всюди: від значків до плакатів. Даний вид графіки дозволяє створити практично будь-яке зображення, незалежно від складності, на відміну від векторної, де неможливо точно передати ефект плавного переходу від одного кольору до іншого без втрат у розмірі файлу. [4]

2.2.1 Огляд растрових форматів зображень

Растрові зображення зазвичай зберігаються в стислому вигляді. Залежно від типу компресії може бути можливо або неможливо відновити зображення таким, яким воно було до цього (стиснення без втрат або стиснення з втратами відповідно).

Так само в графічному файлі може зберігатися додаткова інформація: про автора файлу, фотокамери, її налаштуваннях, кількості точок на дюйм при друці та ін.. [4]

У сучасній комп'ютерній графіці використовуються десятки спеціалізованих форматів даних. Деякі з них розроблені окремими фірмами під конкретні програмні засоби, інші створені науково-дослідними установами, у більшій чи меншій мірі пов'язаними співпрацею з Міжнародною організацією стандартів (iso.org). Проте у повсякденній практиці зустрічається всього лише декілька [4].

На рис.2.3 наведено класифікацію форматів графічних файлів.

Найпростіший формат – BMP (BitMaP, тобто бітова карта), який з'явився з першими версіями операційної системи Microsoft Windows. Він громіздкий, але дозволяє повністю і без втрат створювати копію файлу, при максимальній якості. Аналогічним є формат ICO для зображення у системі Windows так званих іконок – мініатюрних значків-логотипів програм.

Іншим растровим форматом є TIFF (Tagged Image File Format), тобто структурований формат файлу зображення, і саме йому віддають перевагу професіонали. Він був розроблений досить давно, зазнав доповнень, модифікацій та вдосконалень, має велику кількість спеціалізованих варіантів та версій, орієнтованих на всілякі екзотичні галузі, наприклад космічну фотозйомку. Частіше використовується його найпростіший і найнадійніший варіант, без стиснення і втрати даних. Хоча при цьому створюються великі файли, які часом нелегко вмістити на носіях.

Для скорочення витрат на графіку було розроблено спеціальні форми стиснення файлів.

JPG – базується на першому міжнародному стандарті для збереження зображень із деякою втратою якості JPEG (Joint Photographic Expert Group). Стиснення засноване на усередненні кольору сусідніх пікселів (інформація про яскравість при цьому не усереднюється) і відкиданні високочастотних

складових в просторовому спектрі фрагмента зображення. Головним чином він призначений для фото, характерною рисою яких є плавні переходи напівтонів і розмиття чітких ліній.

GIF – формат обміну графікою (Graphic Interchange Format), навпаки, призначений для малюнків з чіткими кольорами та контурами, і економія досягається частково за рахунок мінімізації палітри.

PNG (Portable Network Graphic) – також орієнтований на малюнки з чіткими лініями, але не накладає обмежень на розміри палітри і базується на досконаліших загальнодоступних алгоритмах стиснення даних.

Для зменшення обсягу файлів шляхом усунення фрагментів з повторами даних широко використовуються програми-архіватори, що забезпечують повне збереження «запакованої» інформації. Графічні файли у форматах JPG та GIF практично не стискаються. Зате у десятки разів можуть бути «спресовані» стандартними архіваторами розлогі файли типів BMP або TIF, що зумовлює їх велику розповсюдженість у користуванні. [4]

2.2.2 Огляд колірних моделей

Для задання відповідності між кольорами, що сприймаються людиною та зберігаються в пам'яті, і кольорами, що формуються на пристроях виводу, використовується колірна модель.

Колірна модель – це абстрактна модель опису представлення кольорів у вигляді кортежів (наборів) чисел, зазвичай з трьох або чотирьох значень, що називаються колірними компонентами або колірними координатами. Разом з методом інтерпретації цих даних (наприклад, визначення умов відтворення та/або перегляду – тобто завдання способу реалізації), множина кольорів колірної моделі визначає колірний простір [4].

Колірний простір –це модель представлення кольору, заснована на використанні колірних координат. Кольорова палітра будується таким чином, щоб будь-який колір був представлений точкою, що має певні координати.

Найчастіше одному набору координат буде відповідати один колір, але для деяких випадків це не так.

RGB (Red, Green, Blue – червоний, зелений, синій) – адитивна колірна модель, що описує спосіб синтезу кольору, за якою червоне, зелене та синє світло накладаються разом, змішуючись у різноманітні кольори. Широко застосовується в техніці, що відтворює зображення за допомогою випромінення світла.

Зображена на рис.2.6 та рис.2.4.

У даній моделі колір кодується градаціями складових каналів (Red, Green, Blue). Тому за збільшення величини градації котрогось каналу – зростає його інтенсивність під час синтезу.

Кількість градацій кожного каналу залежить від розрядності бітового значення RGB. Зазвичай використовують 24-бітну модель, у котрій визначається по 8 біт на кожен канал, і тому кількість градацій дорівнює 256, що дозволяє закодувати 2563 = 16 777 216 кольорів. [4]

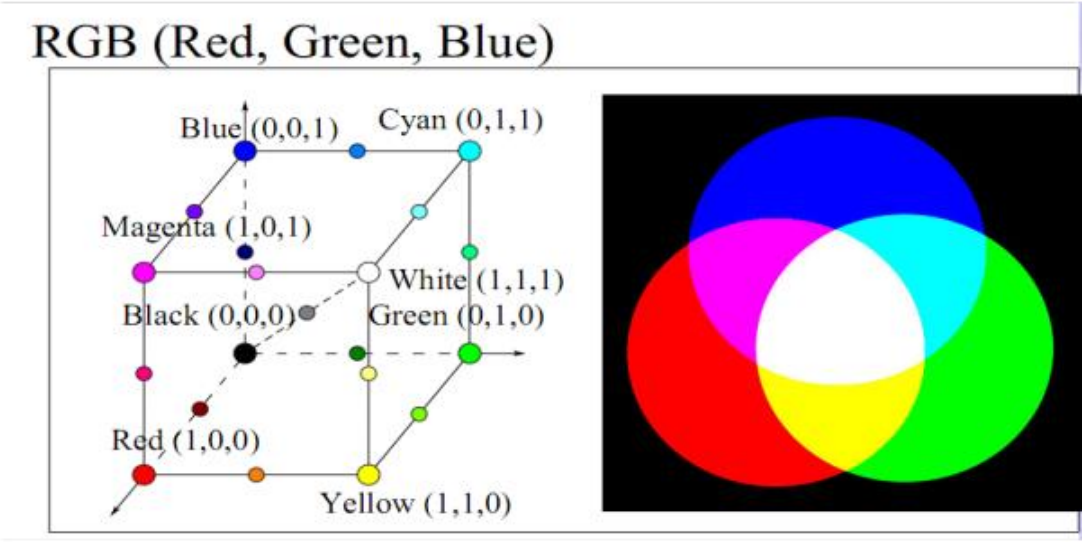


Рис. 2.6. Колірна модель RGB

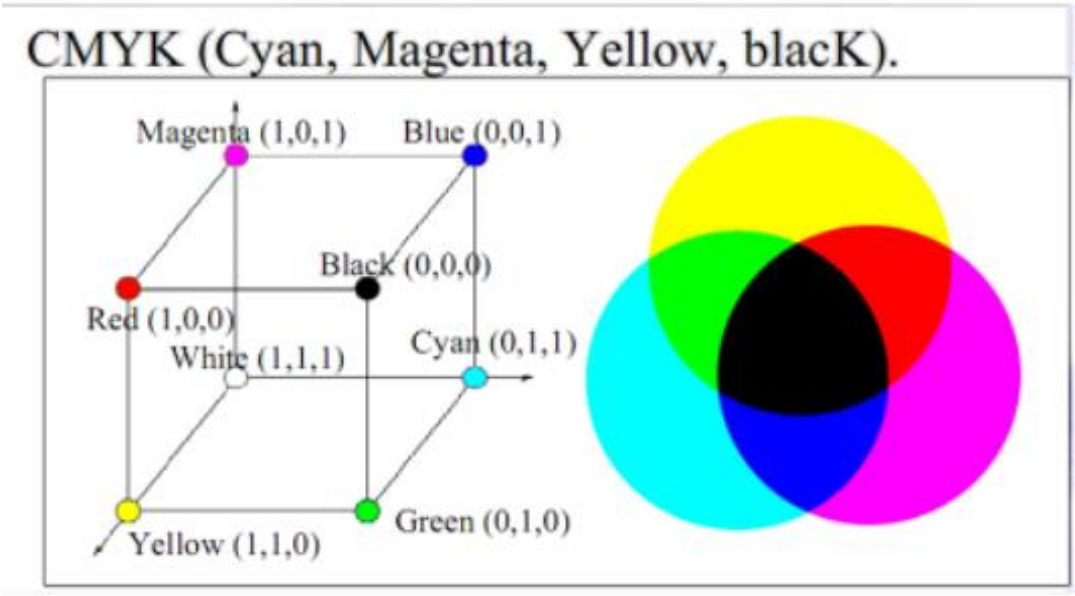


Рис. 2.7. Колірна модель CMYK

Колірна модель RGB призначена сприймати, представляти та відображати зображення в електронних системах, таких як телебачення та комп'ютери, а також її застосовують у традиційній фотографії.

CMYK (Cyan, Magenta, Yellow, BlacK color) – це субтрактивна колірна модель, що використовується у поліграфії, перш за все при повноколірному друці. Вона застосовується у друкарських машинах і кольорових принтерах.

Ця колірна модель зображена на рис.2.7.

Кольори в CMYK описуються сукупністю чотирьох чисел, які також називають колірними координатами. Кожне з цих чисел є відсотком фарби даного кольору у складовій колірної комбінації.

Модель CMYK враховує, яка кількість світла (і кольору) відбилася від тієї або іншої поверхні. Таким чином, якщо відняти з білого три первинні кольори, RGB, отримується трійка доповнюючих кольорів CMY. «Субтрактивний» означає той, що «віднімається». [4]

Модель CMYK забезпечує менше колірне охоплення, ніж адитивна модель RGB.

2.3. Аналіз існуючих методів стеганографії

Підсумовуючи те, що описано в попередніх підрозділах, можна сказати, що комп'ютерна стеганографія базується на двох принципах:

- По-перше, аудіо- та відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без значнго спотворення.
- По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. [3-4]

Базуючись на цьому було сформовано основні методи приховування зображень в стеганографії:

- Методи заміни просторової області;
- Методи приховування частотної області зображення;
- Широкосмугові методи;
- Статистичні методи;
- Методи спотворення;
- Структурні методи. [1]

2.3.1. Методи заміни просторової області

Загальний принцип даних методів полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення. Для відновлення повідомлення необхідно знати алгоритм, за яким розміщувалася в контейнері приховувана інформація. [4]

Найбільш поширеним методом цього типу є метод заміни найменшого значущого біта (НЗБ). Його суть полягає в заміні найменш значущих бітів пікселів зображення бітами секретного повідомлення.

В найпростішому випадку проводиться заміна всіх послідовно розташованих пікселів файлу-контейнера.

Щоб зробити факт приховування менш помітним секретне повідомлення зазвичай доповнюють випадковими бітами так, щоб його довжина в бітах дорівнювала кількості пікселів в оригінальному документі. У такому випадку розподіл змінених пікселів буде рівномірним, а статистичні тести не зможуть виявити будь-які відхилення. [1]

2.3.2. Широкосмугові методи

Широкосмугові методи передачі застосовуються в техніці зв'язку для забезпечення високої завадостійкості і ускладнення процесу перехоплення. Суть широкосмугових методів полягає в значному розширенні смуги частот сигналу, більш ніж це необхідно для передачі реальної інформації. Розширення діапазону виконується в основному за допомогою коду, який не залежить від переданих даних. Корисна інформація розподіляється по всьому діапазону, тому при втраті сигналу в деяких смугах частот в інших смугах присутній достатньо інформації для її відновлення. [3]

Таким чином, застосування широкосмугових методів в стеганографії ускладнює виявлення прихованих даних і їх видалення. Мета широкосмугових методів подібна завданням, які вирішує стегосистеми: спробувати "розчинити" секретне повідомлення в контейнері і унеможливити його виявлення. Оскільки сигнали, розподілені по всій смузі спектра, важко видалити, стеганографічні методи, побудовані на основі широкосмугових методів, є стійкими до випадкових і навмисним перекручуванням.

Для приховування інформації застосовують два основних способи розширення спектра:

- за допомогою псевдовипадкової послідовності, коли секретний сигнал, що відрізняється на константу, модулюється псевдовипадковим сигналом;
- за допомогою стрибаючих частот, коли частота несучого сигналу змінюється за певним псевдовипадковим законом.

Переваги:

- порівняно висока стійкість до спотворень зображення і різного виду атак.

Недоліки:

- нестійкість до стиснення.

2.3.3. Статистичні методи

Статистичні методи приховують інформацію шляхом зміни деяких статистичних властивостей зображення.

Суть методу полягає в такій зміні певних статистичних характеристик контейнера, при яких одержувач зможе відрізнити модифіковане зображення від немодифікованого.

Дані методи відносяться до "однобітових" схемам, тобто орієнтовані на приховування одного біта секретної інформації. l(m) -розрядна статистична стегосистема утворюється з безлічі однорозрядних шляхом розбиття зображення на l(m) блоків $B_1,...,B_{l(m)}$, що не перетинаються. При цьому секретний біт повідомлення вбудовується в і-й блок контейнера. Виявлення прихованого біта в блоці відбувається за допомогою спеціальної функції, яка відрізняє модифікований блок від немодифікованого. [11]

Найчастіше статистичні методи стеганографії складно застосовувати на практиці. По-перше, необхідно мати хорошу статистику $h(B_i)$, на основі якої приймається рішення про те, чи є аналізований блок зображення зміненим чи ні. По-друге, розподіл $h(B_i)$ для "нормального" контейнера має бути заздалегідь відомим, що в більшості випадків є досить складним завданням.

Недоліки:

- неможливість вилучення вбудованої інформації;
- можливість помилкового виявлення ЦВЗ при його відсутності;
- можливість не виявлення ЦВЗ при його присутності.

2.3.4. Методи спотворення

Процес приховування полягає в послідовному виконанні ряду модифікацій контейнера, які вибираються відповідно до секретного повідомлення.

Для вилучення прихованих даних необхідно визначити всі відмінності між стеганограмою та вихідним контейнером.

За цим розбіжностям відновлюється послідовність модифікацій, які виконувалися при приховуванні секретної інформації.

Для приховування даних вибирається l(m) різних пікселів контейнера, які використовуються для приховування інформації. Такий вибір можна зробити, використовуючи датчик випадкових чисел. [1] При приховуванні біта 0 значення пікселя не змінюється, а при приховуванні біта 1 до кольору пікселя додається випадкове значення Δx. Для вилучення секретних даних необхідно провести порівняння всіх l(m) обраних пікселів стеганограми з відповідними пікселями вихідного контейнера. Якщо і-й піксель буде відрізнятися, то це свідчить про те, що в прихованому повідомленні був одиничний біт, інакше - нульовий. [3]

Переваги:

- простота реалізації;
- великий обсяг інформації, яку можна вбудувати.

Недоліки:

- потрібне знання про первісному вигляді зображення-контейнера;
- сильна чутливість до найменших спотворень контейнера.

2.3.5. Структурні методи

По суті, структурні методи є розвитком відомої стеганографічної технології - семаграм. Їх суть полягає в проведенні послідовних перетворень фрагментів графічного файлу, які в кінцевому варіанті призводять до формування приховуваного тексту.

Зараз з'являється безліч графічних пакетів програм і баз даних, за допомогою яких можна створювати різні графічні зображення, презентації, мультиплікацію тощо. У кожному графічному зображенні можна виділити окремі компоненти, які відповідно до його областю інтерпретації мають своє інформаційне навантаження. Візуальний образ S можна представити у вигляді цифрової послідовності, яка потім легко перетворюється в текстове повідомлення. Це можливо, наприклад, в процесі покриття способу деяким

графом, використовуючи інформаційну інтерпретацію його окремих компонентів. У першому наближенні вершинами такого графа можуть бути окремі компоненти малюнка, а ребрами - їх сполуки. При кодуванні інформації, що приховується отриманий граф можна перетворювати досить широким спектром відомих в теорії графів перетворень. В кінцевому варіанті такий граф може бути розмічений відповідно до певного алгоритму і представлений у вигляді його числового інваріанта. Найпростішим інваріантом є матриця суміжності графа. Можна використовувати кілька інваріантів, які описуються в вигляді многочлена. Секретний ключ при такому підході - це спосіб нумерації графа. Відомо, що можлива кількість перенумерованих графів для довільного графа досить велика. Ця обставина робить запропонований спосіб приховування повідомлень досить стійким проти атак на виявлення наявності секретних даних. [1]

У структурних методах можна виділити окремі етапи стеганографічного перетворення.

Першим етапом є перетворення секретного повідомлення m в цифрову форму CH. Це перетворення може бути, наприклад, будь-яким криптографічним перетворенням.

Другий етап являє собою перетворення послідовності чисел CH в графічну структуру GS. В ролі графічних структур найчастіше виступають графи. Окрім графів, можна використовувати різні піктограми або інші структури, які піддаються формальному опису певним чином.

На третьому етапі здійснюється перетворення графічної структури GS у візуально-інформаційне середовище WS. В загальному випадку в якості такого середовища може використовуватися, наприклад, будь-яке мультимедійне або програмне середовище.

Четвертий етап являє собою сукупність методів і відповідних процедур, за допомогою яких формується сюжет із візуальних образів з вбудованими в них секретними повідомленнями.

В рамках даного підходу візуальний образ складається з графічних елементів, які ідентифікуються з елементами GS. Дані елементи являють собою помічені вершини, помічені або непомічені ребра і інші елементи, що ідентифікують компоненти з СН. Необхідним етапом функціонування такої стегосистеми є формування деякого сюжету для фрагмента інформаційного середовища з окремих графічних образів.

Отже, весь ланцюжок перетворень, яка реалізується стегосистемою на рівні окремих етапів перетворення, може бути записана у вигляді: S⇒CH⇒GS⇒WS⇒SJ, де SJ - опис сюжету, який складається з окремих графічних образів. Слід зазначити, що розглянутий підхід можна застосувати як для перетворення зображення з метою розміщення в ньому секретного повідомлення, так і для генерування візуального зображення за секретним повідомленням.

Недоліки:

- необхідність наявності спеціальної мультимедійної або програмного середовища.

Існуючі методи комп'ютерної стеганографії можна класифікувати (рис.2.8), спираючись на публікації [1-3] та вибираючи той чи інший критерій класифікації.

За способом обрання контейнера розрізняють сурогатні, селективні та імітаційні методи стеганографії.

В сурогатних (безальтернативних) методах стеганографії відсутня можливість вибору контейнера і для приховування повідомлення вибирається перший контейнер, що трапився, який у більшості випадків не є оптимальним для приховуваного повідомлення (так званий «ерзац-контейнер»). [1]

У селективних методах КС передбачається, що приховане повідомлення повинно відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велику кількість альтернативних контейнерів,

з наступним обранням (шляхом відбраковування) найоптимальнішого з них для конкретного повідомлення. [3]

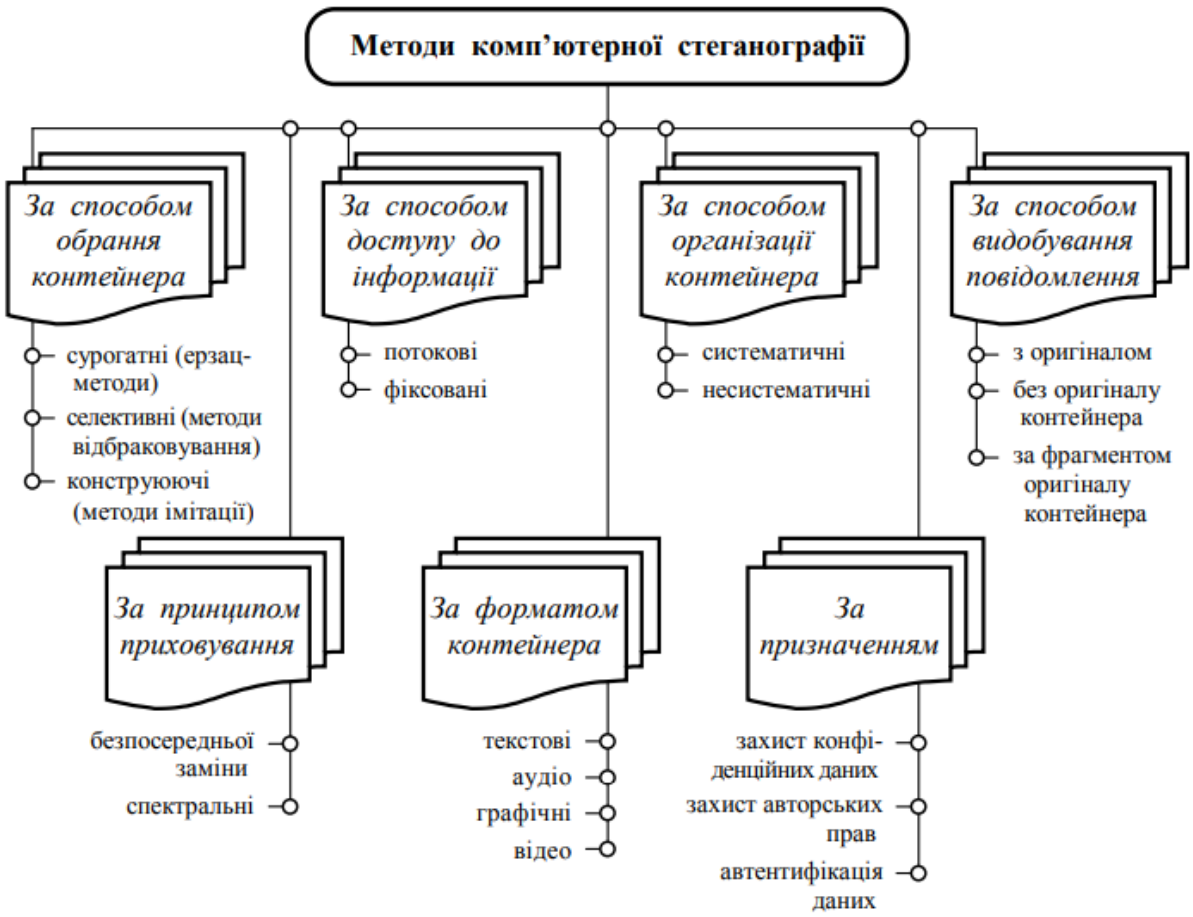


Рис. 2.8. Класифікація методів комп'ютерної стеганографії

Окремим випадком такого підходу є обчислення деякої хеш-функції для кожного контейнера. При цьому для приховування повідомлення обирається той контейнер, хеш-функція якого збігається зі значенням хеш-функції повідомлення (тобто стеганограмою є обраний контейнер).

В імітаційних методах стеганографії контейнер генерується самою стеганосистемою. При цьому існують декілька варіантів реалізації. Так, наприклад, шум контейнера може імітуватися приховуваним повідомленням. Це реалізується за допомогою процедур, які не лише кодують приховане повідомлення під шум, але й зберігають модель початкового шуму. У граничному випадку за моделлю шуму може будуватися ціле повідомлення.

Прикладом може слугувати метод, реалізований у програмі MandelSteg [1], яка в якості контейнера генерує фрактал Мандельброта (Mandelbrot fractal), або ж апарат функцій імітації [3].

За способом доступу до приховуваної інформації розрізняють методи потокових (безперервних) і фіксованих (обмеженої довжини) контейнерів.

За способом організації контейнери, як і завадостійкі коди, можуть бути систематичними і несистематичними. У перших можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти власне контейнера, а де шумові біти, призначені для приховування інформації (як, наприклад, у широко поширеному методі найменшого значущого біту). У випадку несистематичної організації контейнера такий поділ застосувати неможливо. У цьому разі для виділення прихованої інформації необхідно обробляти вміст усієї стеганограми.

За використовуваним принципом приховування методи комп'ютерної стеганографії поділяють на два основних класи: методи безпосередньої заміни та спектральні методи. Якщо перші, використовуючи надлишковість інформаційного середовища в просторовій (для зображення) або часовій (для звуку) області, полягають в заміні малозначимої частини контейнера бітами секретного повідомлення, то другі для приховування даних використовують спектральне представлення елементів середовища, куди вбудовуються приховувані дані (наприклад, до різних коефіцієнтів дикретно-косинусних перетворень, перетворень Фур'є, Карунена-Лоева, Адамара, Хаара тощо). [3]

Основним напрямком КС є використання властивостей саме надлишковості контейнера-оригіналу. Але при цьому треба зважати на те, що при приховуванні інформації відбувається спотворення деяких статистичних властивостей контейнера або ж порушення його структури.

В особливу групу можна виділити методи, що використовують спеціальні властивості форматів представлення файлів [1]:

- зарезервовані для розширення поля файлів, які зазвичай заповнюються нулями і зазвичай не враховуються програмою;
- спеціальне форматування даних (зсування слів, речень, абзаців або обирання визначених позицій літер);
- використання незадіяних ділянок на магнітних та оптичних носіях;
- видалення файлових заголовків-ідентифікаторів тощо.

В основному, для таких методів характерні низький ступінь скритності, низька пропускна здатність і слабка продуктивність.

2.4. Аналіз існуючих програмних рішень стеганографічного приховування графічної інформації

У даному підрозділі аналізується існуюче програмного забезпечення для вбудовування даних у растрові зображення.

2.4.1 Програма Steganos Privacy Suite 11

Програма Steganos Privacy Suite 11 розроблена Steganos Software. Вартість 69,95 $. Дозволяє приховувати дані в растрових зображеннях формату bmp і jpg. Для приховування даних використовується метод НЗБ.

Переваги:

- Дозволяє приховувати файли будь-якого формату;
- Великий обсяг інформації, яку можна приховати;
- Підтримує збереження в форматі JPEG.

Недоліки:

- Не витримує повторне JPEG-стиснення файлу з вбудованими даними.

2.4.2 Програма S-Tools

Програма S-Tools розроблена Анді Брайном (AndyBrown). Дозволяє приховувати дані в зображеннях формату bmp і gif. Для приховування даних використовується метод НЗБ. Розповсюджується безкоштовно.

Переваги:

- Дозволяє приховувати файли будь-якого формату;
- Великий обсяг інформації, яку можна приховати.

Недоліки:

- Немає можливості збереження зображення у форматі jpg;
- Не витримує JPEG-стиснення файлу з вбудованими даними.

2.4.3 Програма ImageSpyer 2009

Програма ImageSpyer 2009 дозволяє приховувати дані в зображеннях формату bmp і tiff. Для приховування даних використовується власна реалізація методу НЗБ. Розповсюджується безкоштовно.

Переваги:

- Дозволяє приховувати файли будь-якого формату;
- Великий обсяг інформації, яку можна приховати.

Недоліки:

- Немає можливості збереження зображення у форматі jpg;
- Не витримує JPEG-стиснення файлу з вбудованими даними.

2.4.4 Програма JSTEG

Програма JSTEG дозволяє приховувати дані у файлах формату jpg. Вона приховує дані в молодших бітах, відмінних від нуля квантованих коефіцієнтів блоків зображення. Розповсюджується безкоштовно.

Переваги:

- Підтримує збереження файлів у форматі jpg;
- Отримані файли витримують JPEG-компресію, але тільки з таблицею квантування аналогічній таблиці, з якою працює програма JSTEG.

Недоліки:

- Орієнтована на роботу в MS-DOS;
- Залежить від таблиці квантування.

2.4.5 Програма Gifshuffle

Програма Gifshuffle дозволяє приховувати дані у файлах формату gif. Приховування інформації проводиться за допомогою зміни порядку кольорів у палітрі. Розповсюджується безкоштовно.

Переваги:

- Можливість попереднього стиснення вбудованих даних.

Недоліки:

- Малий обсяг приховуваного повідомлення, що не залежить від розміру контейнера;
- Не підтримує збереження зображень у форматі jpg.

Порівняння розглянутих стеганографічних програм наведено в таблиці 2.1.

Таблиця 2.1. Порівняння ПЗ для стеганографії

Назва	Формати, що підтримуються	Ціна	Метод приховування
Steganos Privacy Suite 11	*.bmp	69,95$	НЗБ
S-Tools 4	*.bmp, *.gif	-	НЗБ
ImageSpyer 2009	*.bmp, *.tiff	-	НЗБ (власна реалізація)
JSTEG	*.jpg	-	НЗБ у відмінних від нуля квантованих коефіцієнтах блоків зображення
Gifshuffle	*.gif	-	Метод заміни палітри

2.5. Обґрунтування теми дипломного проекту

Як показує практика, за останні декілька років актуальність проблеми інформаційної безпеки невпинно зростала, постійно стимулюючи при цьому пошук нових методів захисту інформації.

Можна виділити три причини популярності досліджень в області стеганографії на сьогодні:

- обмеження на використання крипто-засобів у ряді країн світу,
- появу проблеми захисту прав власності на інформацію, представлену в цифровому вигляді,
- наявність потреби зберігати наявні конфіденційні дані від витоку і розголошення. [4]

Наслідками першої і третьої причин є наявність великої кількості досліджень в дусі класичної стеганографії (тобто приховування факту передачі інформації), другої – ще більш численні праці в області ЦВЗ, ЦП, що дозволяють непомітно вбудовувати секретні повідомлення в зображення (або інші дані) з метою тим або іншим чином контролювати поширення контейнера.

Окрім цього, в останні роки спостерігається збільшення кількості кібератак, зокрема спроб перехоплення конфіденційної інформації, яка передається засобами глобальних інформаційних мереж.

Аналіз існуючої тенденції дає можливість стверджувати, що й в наступні найближчі роки інтерес до впровадження і розвитку методів ефективного захисту інформації тільки зростатиме, чому, зокрема, сприятиме і бурхливий розвиток інформаційних технологій, який ми спостерігаємо сьогодні. [1]

Оскільки з часу зародження комп'ютерної стеганографії пройшло лише 10 років, а як показує історія, час, за який технологія з моменту виникнення досягає стадії поширеного промислового використання, зазвичай становить близько 20 років, можна очікувати в недалекому майбутньому бурхливий розвиток і активне впровадження напрацювань цієї галузі. [3]

Аналіз останніх досліджень і публікацій показав, що найбільшу популярність в комп'ютерній стеганографії здобули методи, що використовують у ролі контейнера зображення. [4]

Проведений аналіз також показав, що однією з ключових проблем стеганографії є питання оптимального використання стегоконтейнера.

А при роботі з даними великого обсягу важливим завданням є прискорення процесів вбудовування та вилучення секретних даних.

Аналізуючи ринок відповідних програмних продуктів, легко побачити, що більшість з них для приховування повідомлень використовують різні модифікації методу НЗБ. Він має низьку стеганографічну стійкість до атак пасивного і активного порушників (зловмисників). Але основним його недоліком є висока чутливість до найменших спотворень контейнера.

Розглянуті програми для здійснення стеганографічного приховування графічної інформації часто дозволяють приховувати лише невелику або обмежену кількість даних.

Часто сучасні стеганографічні методи використовують великі ключі, що заставляє користувачів зберігати їх у вигляді файлів. В такому випадку існує небезпека у викраденні (або втраті) цих файлів. Тому важливим завданням є приведення ключа до такого вигляду, щоб його можна було просто пам’ятати.

Таким чином, актуальним є наукове завдання, що має теоретичне і практичне значення, є розробка нових та удосконалення існуючих стеганографічних методів приховування інформації у зображення. Під удосконаленням методів мається на увазі покращення їхніх якісних або кількісних характеристик.

Вирішення цього завдання дозволить підвищити захищеність передачі секретних даних каналами зв’язку або їх збереження.

2.6. Висновки до розділу

У даному розділі проаналізовано передумови поширеності стеганографії зображень: структурні особливості побудови, психо-візуальну надлишковість інформаційного середовища в просторовій (для зображення) або часовій (для звуку) області.

Проаналізовано також фізіологічні та психофізіологічні особливості зорової системи людини, що створюють підґрунтя для використання стеганографії цифрових зображень.

Проведено аналіз цифрових зображень як потенційних стегоконтейнерів. Розглянуто особливості різних форматів зображень (BMP, JPEG, GIF, PNG, TIFF) та різних колірних моделей (RGB, CMYK). Наведено порівняння векторної та растрової графіки.

На основі цього було обрано для реалізації покращеного методу стеганографії використовувати зображення у форматі BMP в якості контейнера.

Розглянуто класифікацію методів комп'ютерної стеганографії:

- За способом обрання контейнера розрізняють сурогатні, селективні та імітаційні методи стеганографії.

В сурогатних (безальтернативних) методах вибір контейнера є довільним.

У селективних передбачається, що секретне повідомлення повинно відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерується багато альтернативних контейнерів і шляхом відбраковування обирається оптимальний з них для конкретного повідомлення.

В імітаційних методах стеганографії контейнер генерується самою стегосистемою. Так, наприклад, шум контейнера може імітуватися приховуваним повідомленням.

- За способом доступу до секретної інформації розрізняють методи потокових (безперервних) і фіксованих (обмеженої довжини) контейнерів.
- За способом організації контейнери, як і завадостійкі коди, можуть бути систематичними і несистематичними.

У систематичних можна вказати конкретні місця, де знаходяться інформаційні біти власне контейнера, а де шумові біти, призначені для секретної інформації (наприклад, у широко поширеному методі НЗБ).

У випадку несистематичної організації контейнера такий поділ застосувати неможливо. У цьому разі для виділення секретної інформації необхідно обробляти весь вміст.

- За принципом приховування методи комп'ютерної стеганографії поділяють на два основних класи: методи безпосередньої заміни та спектральні методи.

Методи безпосередньої заміни полягають в заміні малозначимої частини контейнера бітами секретного повідомлення.

Спектральні методи для приховування даних використовують спектральне представлення елементів середовища, куди вбудовуються приховувані дані (наприклад, до різних коефіцієнтів дикретно-косинусних перетворень, перетворень Фур'є, Карунена-Лоева, Адамара, Хаара тощо).

Проаналізовано ПЗ для стеганографічного приховування графічної інформації: Steganos Privacy Suite 11, S-Tools, ImageSpyer 2009, JSTEG, Gifshuffle.

Обґрунтовано актуальність стеганографії та необхідність у вдосконаленні її методів. Наведено перелік проблем сучасних методів комп'ютерної стеганографії.

3 МОДИФІКАЦІЯ МЕТОДУ СТЕГАНОГРАФІЇ З ВИКОРИСТАННЯМ МАТРИЦІ СУДОКУ

3.1 Генерація матриці судоку

Квадратна матриця NxN є судоку матрицею, якщо виконуються наступні умови:

- Для заповнення матриці використовується лише заданий набір з N цифр,
- Цифри в межах кожного з рядків унікальні,
- Цифри в межах кожного з стовпчиків унікальні,
- Цифри в межах кожного з районів унікальні (Матриця послідовно ділиться на райони – квадрати зі сторонами sqrt(N))

Завдяки четвертому правилу побудови судоку, спотворення стегоконтейнера виглядають непомітними для ока людини.

Розглянемо процедуру генерації судоку матриці при N=9. Аналогічно можна формувати матриці судоку будь-яких інших розмірностей (16x16, 256x256, …).

Процедуру генерації матриці можна розбити на два кроки:

1). Утворення «базової матриці»

За основу майбутньої матриці беремо «базову матрицю», вона повинна відповідати всім правилам формування матриці судоку.

Розміщуємо в першому рядку цифри: 1, 2 ... 9, а в рядках нижче зміщуємо на 3 позиції вліво, тобто записуємо цифри: 4 5 ... 2, 3 і 7 8 ... 5 6.

Далі переходячи в наступний район по вертикалі зміщуємо на 1 позицію вліво попередній район.

В результаті таких дій утворюється матриця як на Рис.3.1

1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	1	2	3
7	8	9	1	2	3	4	5	6
2	3	4	5	6	7	8	9	1
5	6	7	8	9	1	2	3	4
8	9	1	2	3	4	5	6	7
3	4	5	6	7	8	9	1	2
6	7	8	9	1	2	3	4	5
9	1	2	3	4	5	6	7	8

Рис.3.1. “Базова матриця” судоку, що використовується у представленій програмі

2). Перемішування елементів матриці

Існує декілька видів перестановок, після виконання яких матриця судоку залишається коректною (відповідає правилам формування матриці судоку).

До них належать:

1. Транспонування всієї матриці (коли стовпці стають рядками і навпаки). Рис.3.2.;

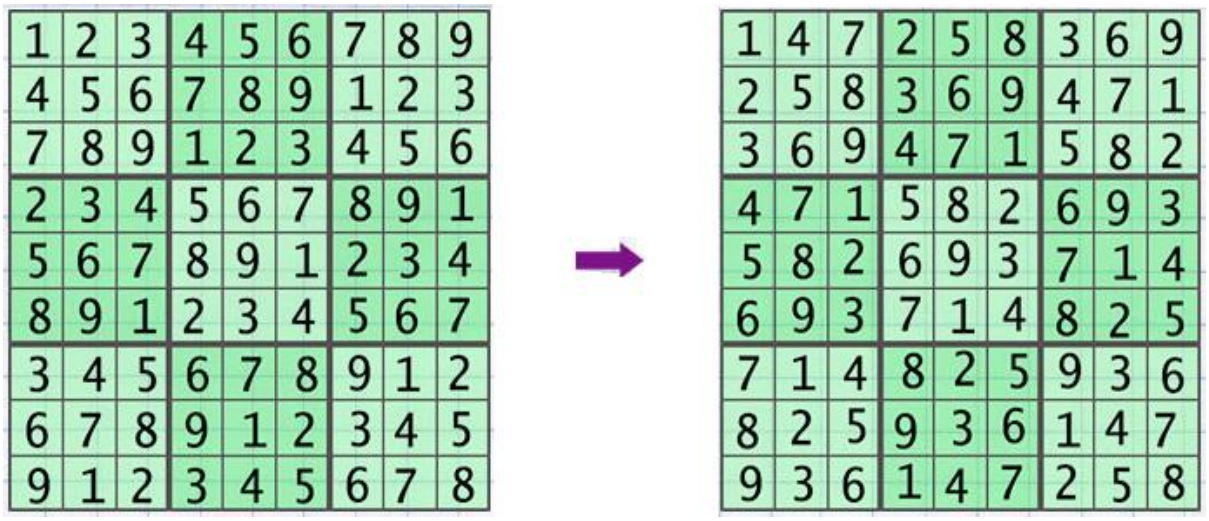


Рис.3.2. Транспонування «базової матриці»

2. Обмін двох рядків в межах одного району (Рис.3.3);

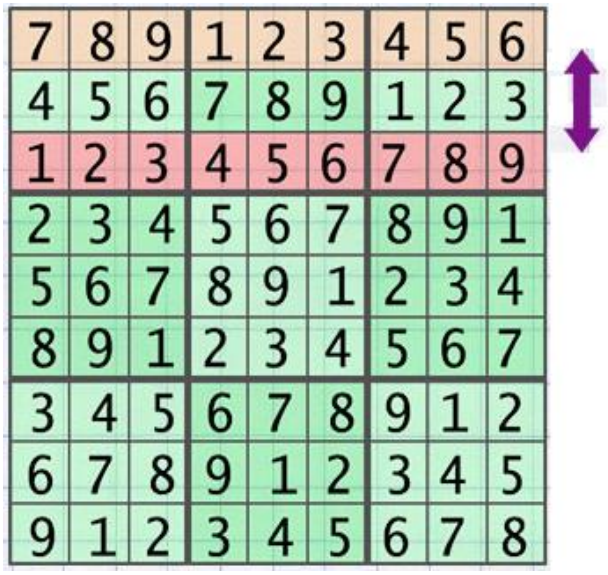


Рис.3.3 Обмін двох рядків в межах одного району «базової матриці»

3. Обмін двох стовпців у межах одного району (Рис.3.4);

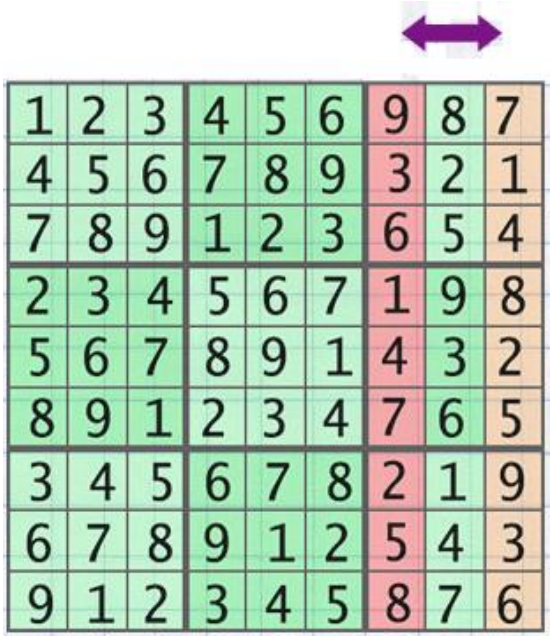


Рис.3.4. Обмін двох стовпців у межах одного району «базової матриці»

4. Обмін двох районів по горизонталі (Рис.2.5 (зліва));
5. Обмін двох районів по вертикалі (Рис.2.5 (справа));

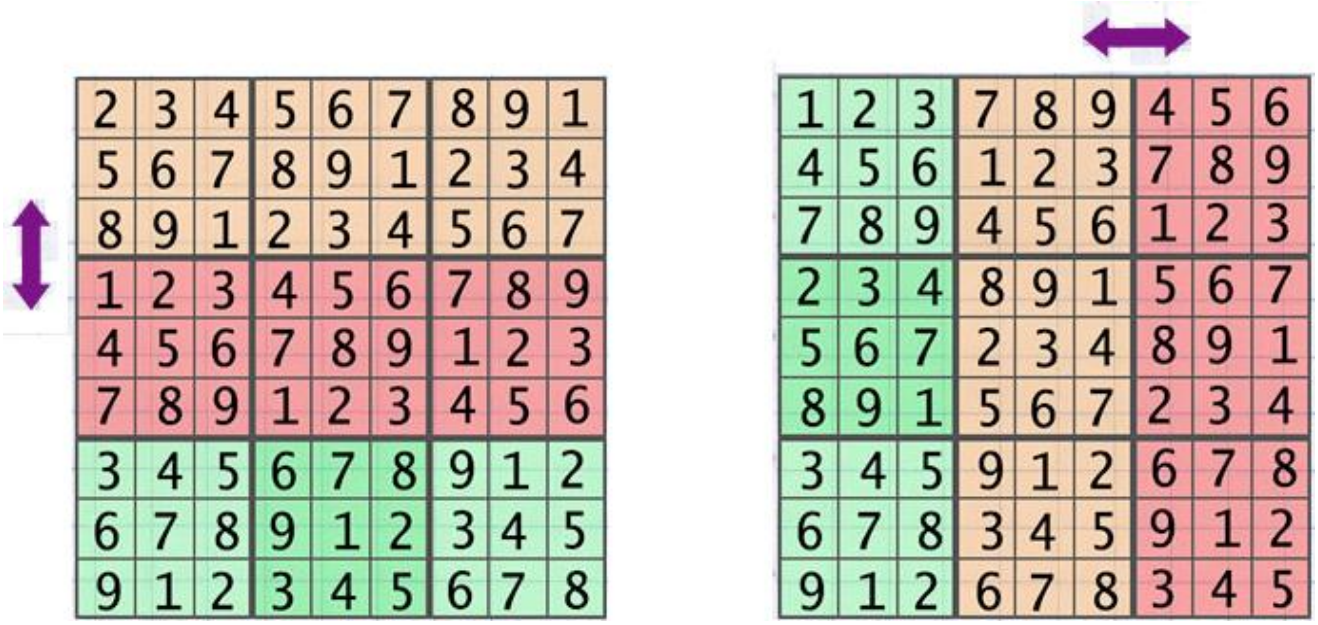


Рис.3.5. Обмін двох районів по горизонталі (зліва) та по вертикалі (справа) «базової матриці» судоку

Це не всі перестановки, після яких матриця судоку залишається коректною. Але ми обмежимося цими. Цей «каркас» є інваріантним до своєї структури, такі перестановки є майже тим самим, що і дії над матрицями щодо визначника або складання Кубика Рубика.

Для того щоб отримати випадкову комбінацію, достатньо лише запустити у випадковому порядку функції перемішування.

3.2 Кодування даних методом стеганографії з використанням судоку матриці

В якості контейнера пропонується використовувати зображення у форматі .bmp з глибиною 24.

Розглянемо процедуру формування стеганографічного ключа. Для кодування інформації використовується ключ - коректно заповнена двовимірна матриця судоку. Процедуру заповнення матриці судоку описано у п.2.3 «Заповнення матриці судоку». Розмір матриці - 9 на 9, числа для заповнення - від 0 до 8. Отриману матрицю дублюється так, щоб отримати нову матрицю розміром 256 на 256. [24]

Підготовка секретного повідомлення (зображення) до кодування полягає в тому, що перед кодуванням секретні дані необхідно привести до певного

вигляду. Для цього ми значення кожного байту подаємо у вигляді 3-ох значного числа у системі числення за основою 9. [7]

Після того, як стеганографічний ключ отримано, а секретне повідомлення підготовлено, можна розпочинати кодування даних.

Алгоритм кодування даних зображено на Рис.3.6.

Для цього беремо перший байт секретних даних (3-ох значне число за основою 9), зчитуємо першу цифру.

Беремо 2 пікселі картинки-контейнера. Зчитуємо значення байтів у R складовій пікселів - отримані значення слугуватимуть початковою X та Y координатою у матриці судоку розміром 256 на 256.

Знаходимо найближчі координати до X та Y, значення комірки в якій рівне значенню зчитаної цифри.

Друга цифра секретного байту кодується в G складову пікселів, третя цифра - у B складову. Таким чином ми можемо закодувати усі секретні дані в наступні пікселі картинки контейнера.

Розглянемо на прикладі процес кодування даних. Для цього формуємо матрицю судоку 9 на 9 заповнену числами від 0 до 8. Продублювавши її, отримуємо матрицю 256 на 256.

Підготуємо секретні дані для кодування. Нехай необхідно закодувати число 216, тоді: $216_{10}=260_9$.

Для кодування числа необхідно «приховати» всі його три цифри.

Для кодування першої цифри зчитуємо цифру "2". Беремо два пікселі з картинки-контейнера і зчитуємо їх R складові. Ці значення відповідатимуть X та Y координатам у матриці судоку 256 на 256.

В матриці 256 на 256 шукаємо найближчу комірку, відносно комірки з координатами X та Y, значення в якій дорівнює "2".

X та Y координати цієї комірки записуємо в R складові обраних пікселів (в картинку-контейнер).

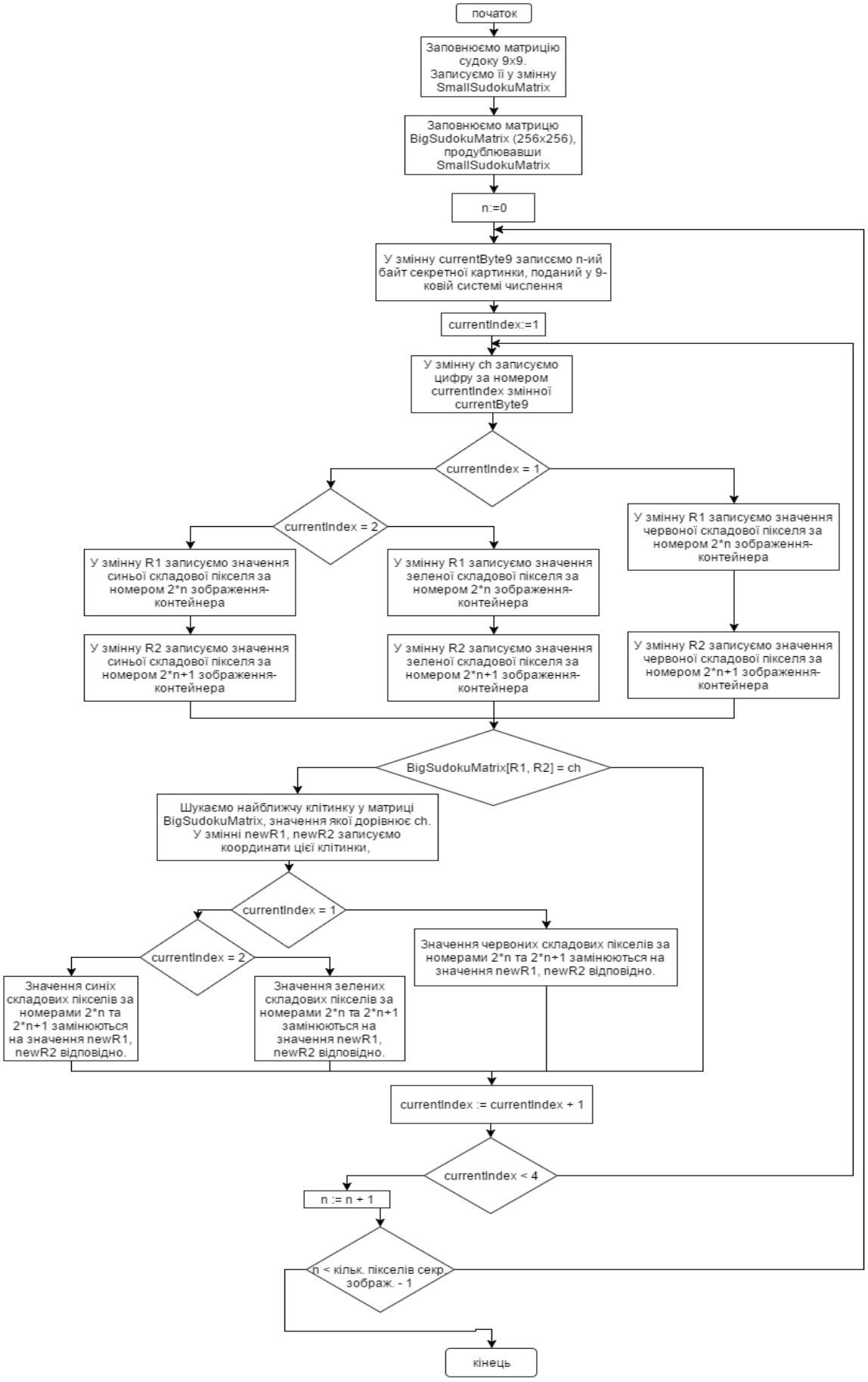


Рис.3.6 Алгоритм кодування даних з використанням судоку матриці

Для кодування другої цифри зчитуємо цифру "6". Зчитуємо G складові пікселів. Ці значення відповідатимуть X та Y у матриці судоку 256 на 256.

В матриці 256 на 256 шукаємо найближчу комірку, відносно комірки з координатами X та Y, значення в якій дорівнює "6".

X та Y координати цієї комірки записуємо в G складові обраних пікселів контейнера.

Аналогічно для кодування третьої цифри зчитуємо цифру "0". Зчитуємо B складову пікселів. Ці значення відповідатимуть X та Y у матриці судоку 256 на 256.

В матриці 256 на 256 шукаємо найближчу комірку, відносно комірки з координатами X та Y, значення в якій дорівнює "0".

X та Y координати цієї комірки записуємо в B складові обраних пікселів зображення-контейнера.

Таким чином ми закодували один секретний байт у двох пікселях картинки-контейнера. Наступні секретні байти записуватимуться в наступні пікселі картинки-контейнера за аналогічним принципом (як описано вище).

3.3 Декодування даних методом стеганографії з використанням судоку матриці

Для декодування інформації в якості ключа береться двовимірна матриця судоку, що була використана для кодування даного зображення. (Розмір матриці - 9 на 9, числа для заповнення - від 0 до 8.) Отриману матрицю дублюється так, щоб отримати нову розміром 256 на 256. [7][24]

Тепер можна розпочинати декодування даних.

Детальний алгоритм декодування даних зображено на Рис.3.7.

Для цього беремо 2 пікселі закодованої картинки. Зчитуємо значення байтів у R складової пікселів. Ці значення слугуватимуть X та Y координатою у матриці судоку розміром 256 на 256.

Зчитавши значення комірки за координами X та Y у судоку матриці, ми отримали першу цифру секретного байту.

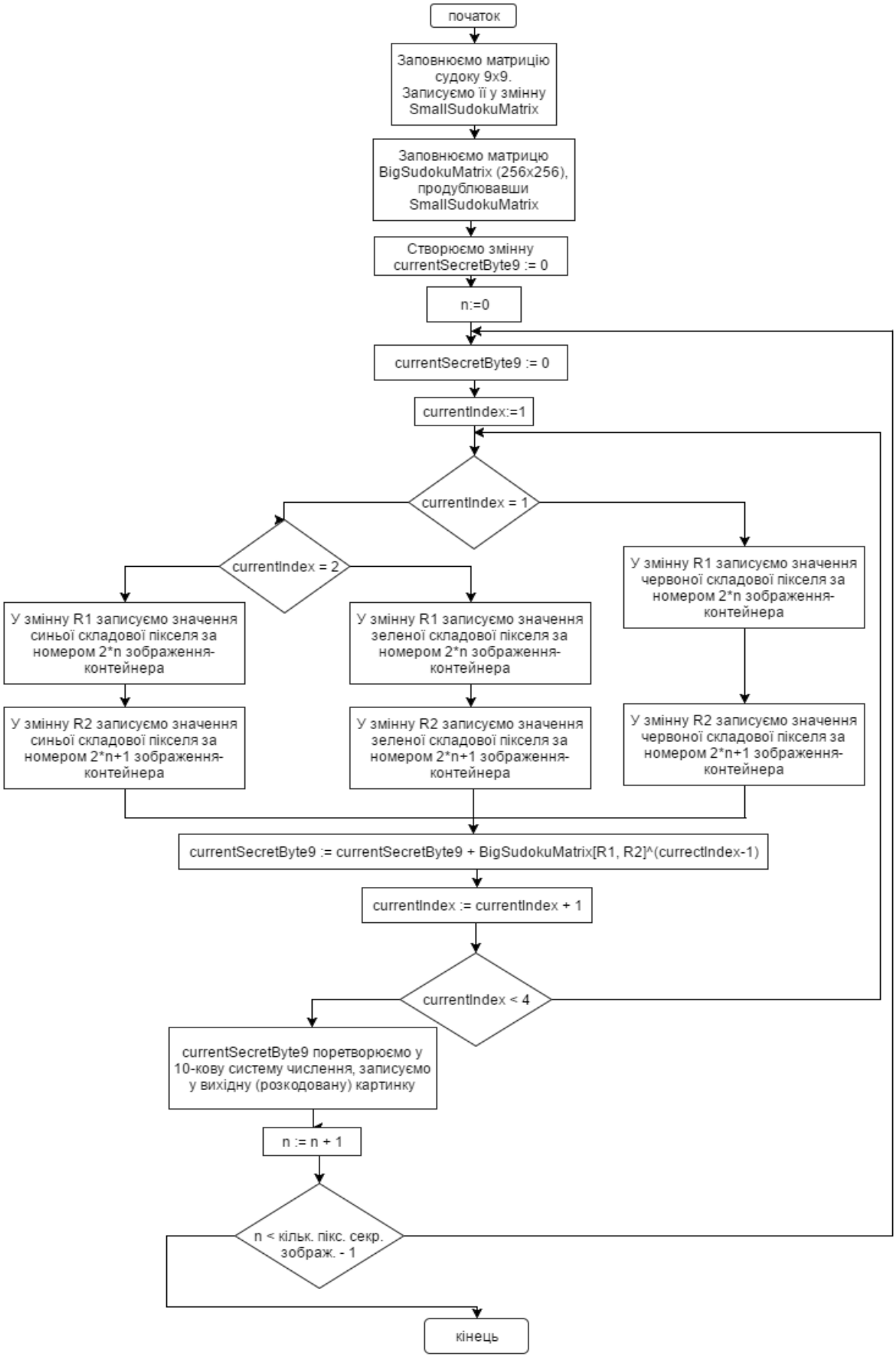


Рис.3.7. Алгоритм декодування даних з використанням судоку матриці

Друга цифра секретного байту отримується аналогічно із G складової цих пікселів, третя цифра - із B складової.

Повторивши ці дії для усіх пікселів секретної картинки зможемо отримати секретне зображення.

3.4 Модифікації методу стеганографії з використанням судоку матриці

В даній науковій роботі було проведено дослідження можливості підвищення ефективності роботи методу стеганографічного приховування інформації за допомогою ключа у вигляді матриці судоку. Для цього нами було проаналізовано основні кількісні характеристики, які впливають на ефективність використання об'єму стегоконтейнера (для підвищення щільності розміщення секретних даних), а також на швидкість роботи алгоритмів кодування та декодування. Основною задачею даної роботи стала така модифікація існуючого алгоритму кодування і декодування, яка дозволить збільшити кількість байтів секретної інформації всередині стегоконтейнера, зменшити кількість елементарних операцій, які необхідно виконати для кодування та запису секретних даних всередину зображення-контейнера, а також зчитування і відновлення секретної інформації після декодування.

У класичному стеганографічному методі кодування та декодування секретної інформації, який був розглянутий у попередніх підрозділах, в якості секретного ключа використовувалася матриця судоку, розмірністю 9 на 9. Для підвищення місткості стегоконтейнера, двійкова матриця ключа була збільшена до розмірності 256 на 256.

В результаті такої модифікації нам вдалося приховати 1 байт секретної інформації в стегоконтейнері, використовуючи лише одну із складових (R, G або B) двох сусідніх пікселів, на відміну від класичного метода стеганографії, в якому для кодування 1 байта секретної інформації використовувалися всі 3 складові (R, G та B) сусідніх пікселів. Таким чином нам вдалося досягнути трьохкратного підвищення пропускної здатності в покращеному методі стеганографії.

Таблиця 3.1 Основні характеристики та відмінності класичного та покращеного методу стеганографії з використання матриці судоку

	Класичний метод стеганографії з використанням матриці судоку	Покращений метод стеганографії з використанням матриці судоку
Кількість секретних байтів, які можуть бути приховані в 2 пікселях стегоконтейнера	1	3
Пропускна здатність методу	1/6	1/2
Необхідність перетворення секретних даних з одної системи числення в іншу перед кодуванням	так	ні
Необхідність перетворення секретних даних з одної системи числення в іншу після декодування	так	ні

Ще одним важливим покращенням запропонованого методу є те, що завдяки збільшенню ключа у нас відпадає необхідністю у перетворенні секретних даних до інших систем числення, як це відбувалося у класичному методі стеганографії. Для роботи з даними по класичному методу нам необхідно було трансформувати дані до тієї системи числення, яку допускала матриця 9 на 9. У покращеному методі ми маємо змогу кодувати секретні дані одразу в такому ж форматі, в якому вони потрапляють до нас. Те ж саме відбувається під час процесу зчитування секретної інформації - дані, які ми

отримуємо в результаті декодування стегоконтейнера з використанням матриці судоку 256 на 256 можуть бути одразу ж опрацьовані або збережені на диск без будь-яких додаткових перетворень.

Основні характеристики та відмінності між класичним та покращеним методом стеганографії з використанням матриці судоку наведено у таблиці 3.1.

3.5 Кодування даних модифікованим методом стеганографії з використанням судоку матриці

В якості контейнера пропонується використовувати зображення у форматі .bmp.

Розглянемо процедуру формування стегоключа. На відміну від класичного варіанту методу, для кодування інформації модифікованим методом в якості ключа використовується двовимірна матриця судоку, розміром 256 на 256, числа для заповнення - від 0 до 255. Процедуру заповнення матриці судоку описано у п.3.1, а процедуру генерації стегоключа за паролем - у п.3.7.

Підготовка секретного повідомлення до кодування полягає в тому, що перед кодуванням секретних даних їх необхідно перетворити у масив байтів, а також зберегти інформацію про розмір цього масиву. При кодуванні файла також необхідно зберегти його назву та її довжину.

Наступним кроком йде перевірка чи зображення-контейнер має достатній розмір для приховування всього масиву секретних байтів. Для цього нам потрібно підрахувати, скільки місця необхідно для збереження службової інформації про секретні дані (розмір масиву байтів, назва файла, довжина назви файла) і, власне, самих секретних даних.

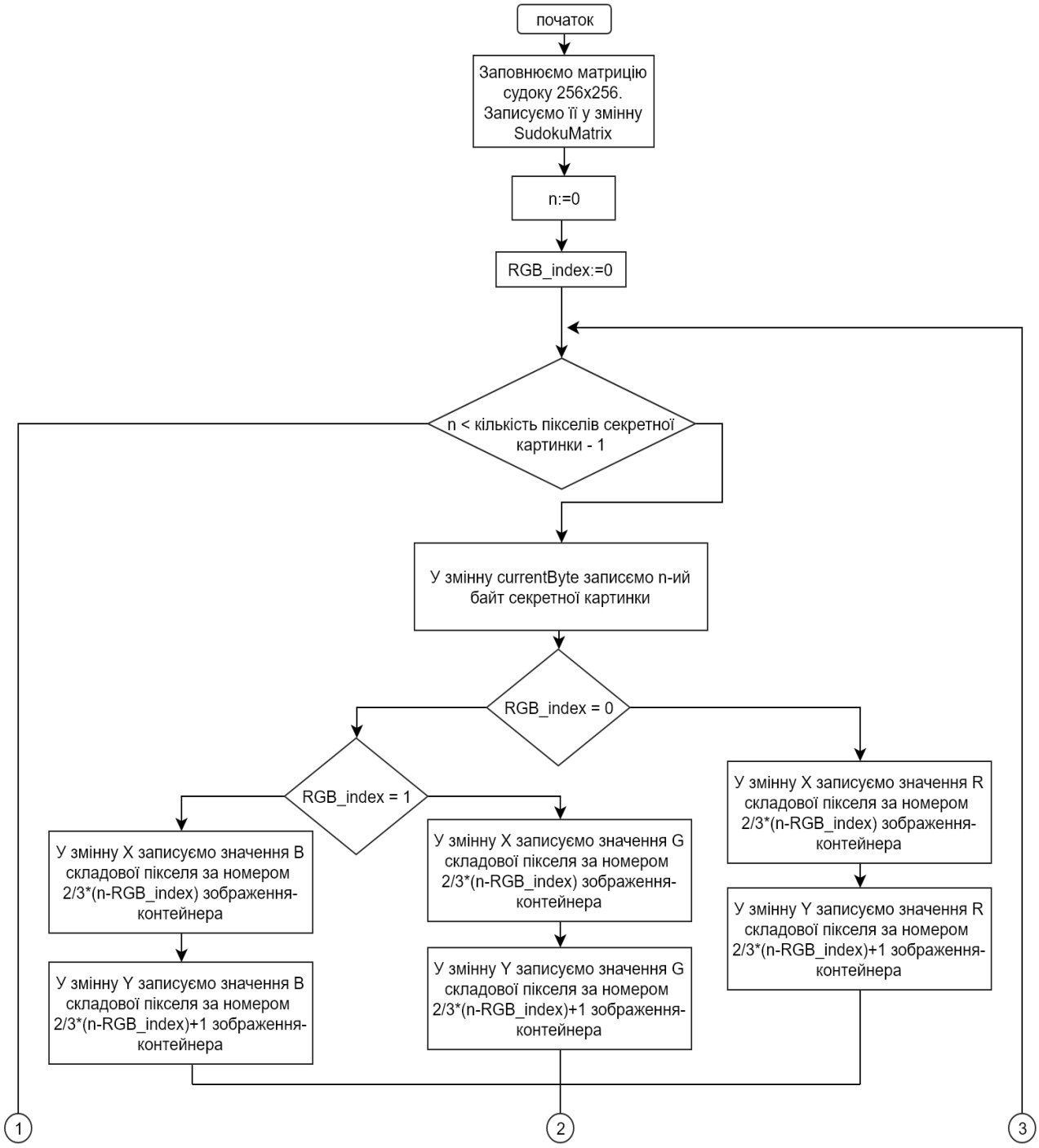


Рис.3.8. Модифікований алгоритм кодування даних з використанням судоку матриці. Частина-1

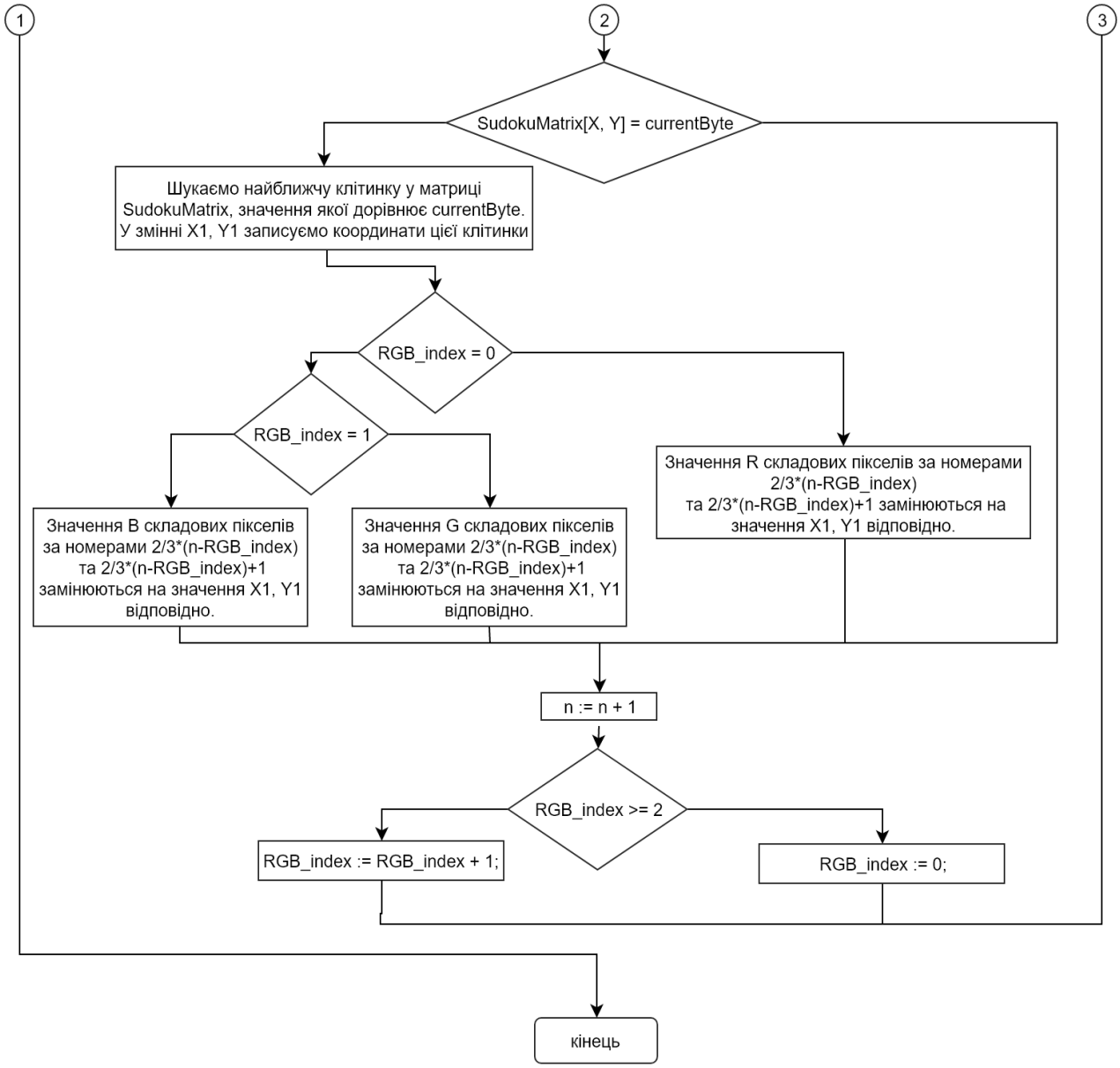


Рис.3.9. Модифікований алгоритм кодування даних з використанням судоку матриці. Частина-2

В модифікованому алгоритмі у 2 пікселі стегоконтейнера можна вбудувати 3 байти секретної інформації, на відміну від класичного методу, в результаті роботи якого в 2 пікселях стегоконтейнера вдавалося розмістити лише 1 байт секретних даних.

Відповідно, сума байтів для збереження службової інформації і секретних даних не повинна перевищувати 3/2 від загальної кількості пікселів стегоконтейнера.

Після того, як стегоключ отримано, секретне повідомлення підготовлено (подано у вигляді масиву байтів), а розмір стегоконтейнера є достатнім, для розміщення усіх байтів, можна розпочинати кодування даних.

Модифікований алгоритм кодування даних з використанням судоку матриці розміром 256 на 256 зображено на рис.3.8 та рис. 3.9.

Розглянемо на прикладі процес кодування секретних даних. Для цього формуємо матрицю судоку 256 на 256 заповнену числами від 0 до 255.

Підготуємо секретні дані для кодування. Нехай необхідно закодувати масив байтів зі значеннями [116, 24, 253].

Для кодування першого байта секретних даних беремо два перші пікселі із зображення-контейнера і зчитуємо їх R складові. Ці значення відповідатимуть X та Y координатам у матриці судоку 256 на 256.

У матриці 256 на 256 шукаємо найближчу комірку, відносно комірки з координатами X та Y, значення в якій дорівнює "116".

X та Y координати цієї комірки записуємо в R складові обраних пікселів (в зображення-контейнер).

В результаті роботи алгоритму для приховування даних ми закодували один секретний байт у R складовій двох пікселів зображення-контейнера.

Наступні два секретні байти записуватимуться в G і B складові першого пікселя зображення-контейнера за аналогічним принципом (як описано вище). Таким чином ми можемо в будь-яких двох пікселях зображення-контейнера приховати по 3 байти секретної інформації. Процедура приховування секретних даних продовжується до тих пір, поки весь масив байтів з секретної інформацією не буде закодовано в стегоконтейнері.

3.6 Декодування даних модифікованим методом стеганографії з використанням судоку матриці

Для декодування інформації в якості ключа береться двовимірна матриця судоку, що була використана для кодування даного зображення. (Розмір матриці - 256 на 256, числа для заповнення - від 0 до 255).

Отримавши матрицю, можна розпочинати декодування даних.

При декодуванні перші байти секретного повідомлення будуть містити деяку службову інформацію: назву файлу, його довжину і тд.. На основі цього ми знаємо, коли слід зупинити процес декодування.

Для цього беремо 2 пікселі закодованого зображення і зчитуємо значення R складових даних пікселів. Ці значення слугуватимуть X та Y координатою у матриці судоку розміром 256 на 256.

Зчитавши значення комірки у судоку матриці за координатами X та Y, ми отримали значення першого байту секретної інформації. Знайдене значення зберігається в результуючий масив байтів з секретними даними.

Другий і третій секретні байти знаходиться аналогічно із G та B складових даних пікселів.

Беремо ці ж 2 пікселі закодованого зображення. Зчитуємо значення G складових даних пікселів. Вони слугуватимуть X та Y координатою у матриці судоку розміром 256 на 256 відповідно.

Зчитавши значення комірки за координатами X та Y у судоку матриці, ми отримали значення наступного (другого) байту секретної інформації. Додаємо знайдене значення в результуючий масив байтів із секретних даних.

Після цього зчитуємо значення B складових цих двох пікселів. Аналогічно, ці значення слугуватимуть X та Y координатою у матриці судоку 256 на 256.

Отримавши значення комірки за координатами X та Y у судоку матриці, отримується значення третього байту секретної інформації. Тому додаємо його в результуючий масив байтів секретних даних.

Далі опрацьовуємо пікселі за номерами 3 та 4 заповненого стегоконтейнера.

Повторюючи такі дії для усіх наступних пікселів зображення-контейнера ми зможемо отримати весь масив байтів із секретною інформацією, яка була вбудована в нього раніше.

Детальний алгоритм декодування даних зображено на рис.3.10.

Рис. 3.10 Модифікований алгоритм декодування даних з використанням судоку матриці

3.7 Генерація стегоключа за паролем

Через те, що судоку матриця є складною для запам’ятовування, є небезпека того, що стегоключі зберігатимуть на електронних носіях, що створює загрози їх випадкової втрати або викрадення.

Зважаючи на ці проблеми, було вирішено розробити спосіб генерації стегоключа використовуючи звичайний пароль.

Відповідно до рекомендацій щодо стійкості паролів, було визначено обмеження на довжину: мінімум 8 символів, максимум – 20.

Розглянемо алгоритм генерації стегоключа за паролем.

Спочатку генеруємо хеш-код пароля, введеного користувачем.

Система генерації стегоключа (матриці судоку) містить базову матрицю судоку та функції, що реалізовують чотири еквівалентні перетворення судоку матриці (див. підрозділ 3.1).

Опрацьовуємо отриманий хеш-код посимвольно. Над кожним значенням символа хеш-коду беремо остачу від ділення ASCII-коду символа на 4 (максимальна кількість реалізованих еквівалентних перетворень матриці судоку) і виконуємо відповідне еквівалентне перетворення над матрицею.

Описаний алгоритм зображено на рис.3.11.

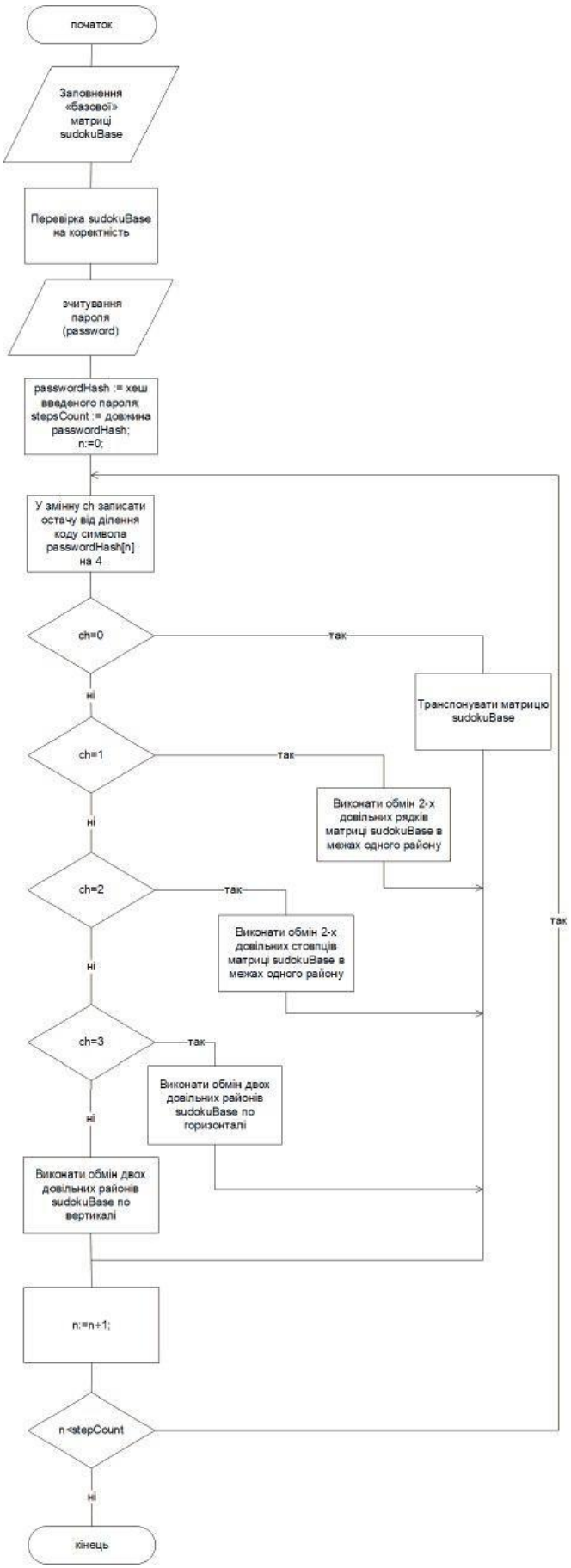


Рис.3.11. Алгоритм генерації стегоключа (матриці судоку) за паролем

3.8 Висновки до розділу

В результаті проведеного дослідження було розроблено модифікацію для методу стеганографії з використанням матриці судоку. Шляхом зміни розмірності матриці, яка слугує ключем для кодування та декодування секретних даних, вдалося досягнути значного збільшення пропускної здатності стегоконтейнера. Покращений метод стеганографії дозволяє приховувати в каналах R, G та B двох обраних пікселів 3 байти секретної інформації. У класичному алгоритмі, який використовує ключ розмірністю 9 на 9, в кольорових каналах двох пікселів можна приховати лише 1 байт секретної інформації. Застосування секретного ключа з розмірністю 256 на 256 дозволило нам раціональніше використати пікселі зображення-контейнера.

Важливою особливістю покращеного методу стеганографії також є те, що секретну інформацію, подану у вигляді масиву байт, не потрібно додатково перетворювати перед початком кодування. Також, після декодування, отримані дані одразу ж можуть бути використані та опрацьовані, або збережені у файл. В класичному методі будь-яку вхідні дані спершу потрібно було перетворювати до системи числення за основою 9, відповідно, при декодуванні секретних даних доводилося виконувати зворотній процес перетворення. Можливість працювати з масивом байтів секретних даних без будь-якого додаткового перетворення дозволяє значно зменшити кількість операцій при шифруванні та дешифруванні, що дозволяє прискорити роботу нового методу.

Отже, модифікований метод відрізняється від існуючого покращенням якісних показників стегосистеми - пропускної здатності та складності вбудовування і вилучення секретного повідомлення.

Для підвищення надійності та зручності розробленої системи стеганографічного приховування інформації було вирішено виконувати генерацію стегоключів (матриць судоку) шляхом використання паролів.

4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ РІШЕНЬ СТЕГАНОГРАФІЇ

На основі аналізу цифрових зображень (п.2.2) для досліджень були обрані зображення формату bmp, оскільки даний формат не підтримує компресії.

Враховуючи особливості роботи ЗСЛ (описані у п.2.1), можна запобігти виявленню факту наявності секретних даних методом візуальної атаки, оскільки вона заснована на здатності ЗСЛ аналізувати зорові образи й виявляти спотворення у зображеннях.

Відповідно до п.2.1, рекомендується використовувати в якості контейнера зображення без різких переходів між його областями та з великою кількістю дрібних деталей.

Для оцінки стійкості даного методу до візуальних атак (непомітність вбудовування) було проведено усне опитування, в якому взяли участь 10 респондентів. Для опитування було підготовлено 20 заповнених зображень-контейнерів різного типу і 10 звичайних зображень, серед яких лише 4 зображення викликали підозри.

4.1 Аналіз та приклади роботи розробленої системи

Проаналізуємо результати роботи розробленої системи стеганографічного приховування інформації:

а) В даному прикладі використовується контейнер №1 та секретне зображення №1.

В якості контейнера використовується зображення розміром 3456x2304, глибиною кольору: 24 біти. Воно містить велику кількість дрібних деталей та плавні переходи між текстурними областями.

На рис. 4.1 зображено незаповнений контейнер, на рис. 4.2 зображено заповнений контейнер, на рис. 4.3 зображено секретне зображення, яке було вбудовано, а потім відновлено. Розмір секретного повідомлення становить 78,2 КВ.

Відповідно до опитування, заповнений контейнер не викликає підозр.

На рис.4.4 наведено порівняння незаповненого контейнера №1 (з рис.4.1) та заповненого контейнера №1 (з рис.4.2) при збільшенні у 8 разів. Як видно, навіть при такому збільшенні дуже важко помітити хоч якісь спотворення, що виникають в результаті вбудовування секретної інформації.

Рис. 4.1 Незаповнений контейнер №1

Рис. 4.2 Заповнений (секретним зображенням №1, рис.4.3) контейнер №1

Рис. 4.3 Секретне зображення №1

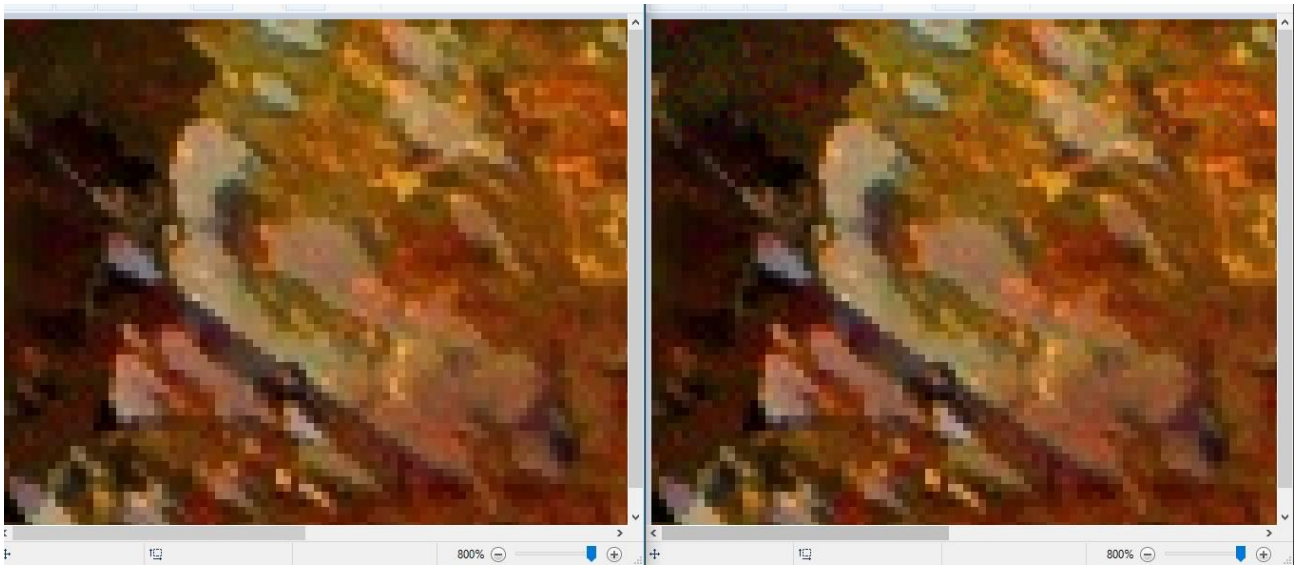


Рис.4.4 Незаповнений (зліва) та заповнений (справа) контейнер №1 при збільшенні у 8 разів

b) В даному прикладі використовується контейнер №2 та секретне зображення №2.

В якості контейнера використовується зображення розміром 1140x550 та глибиною кольору: 24 біти. Воно містить розмиті області та зовсім невелику кількість дрібних деталей.

На рис. 4.5 зображено незаповнений контейнер, на рис. 4.6 зображено заповнений контейнер, на рис. 4.7 - секретне зображення, яке було вбудовано, а потім відновлено. Розмір секретного повідомлення становить 34,9 КВ.

Під час проведення опитування у однієї людини з десяти виникли підозри стосовно заповненого контейнера.

На рис.4.8 наведено порівняння першого фрагменту незаповненого контейнера №2 (з рис.4.5) та заповненого контейнера №2 (з рис.4.6) при збільшенні у 8 разів. При такому збільшенні можна помітити, що заповнений контейнер містить невеликі спотворення. Але інший фрагмент незаповненого і заповненого контейнерів (рис. 4.9) навіть при великому збільшенні не викликає підозр. Відмінність цих фрагментів полягає в тому, що перший складається з однотонної області без будь-яких деталей (розмитий фон зеленого кольору), а інший – містить дрібні елементи різного кольору без різких переходів (фрагмент крила пташки).

Рис. 4.5 Незаповнений контейнер №2

Рис. 4.6 Заповнений (секретним зображенням №2, рис.4.7) контейнер №2

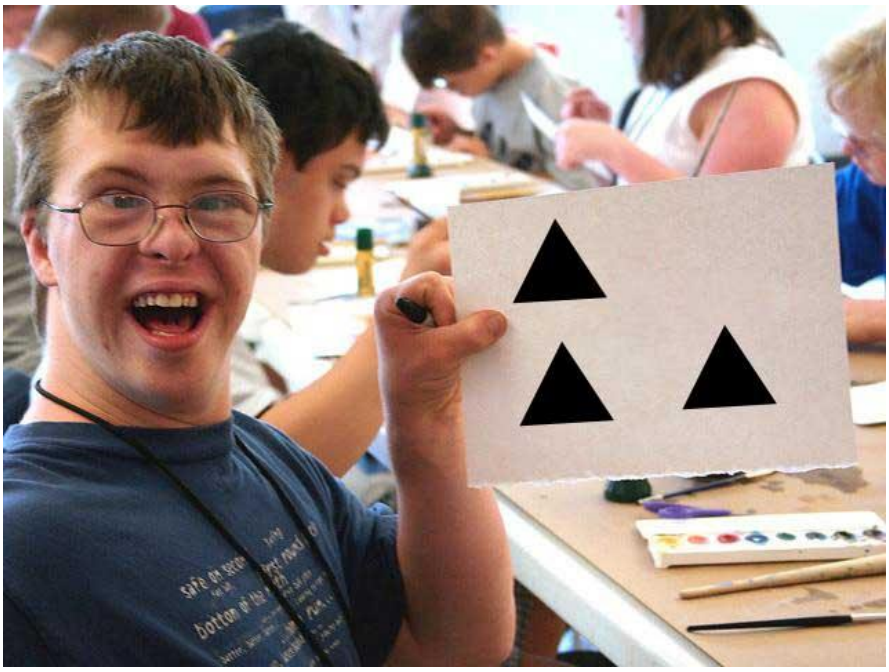


Рис. 4.7 Секретне зображення №2

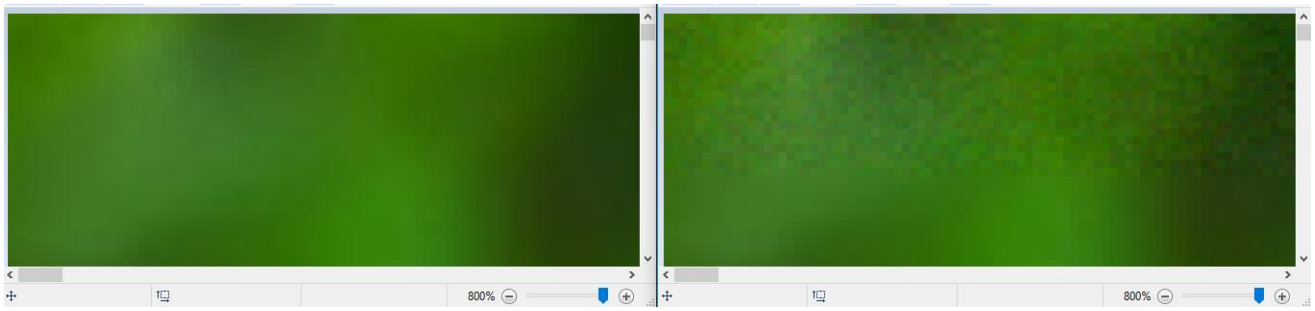


Рис.4.8 Незаповнений (зліва) та заповнений (справа) контейнер №2 при збільшенні у 8 разів. Фрагмент №1

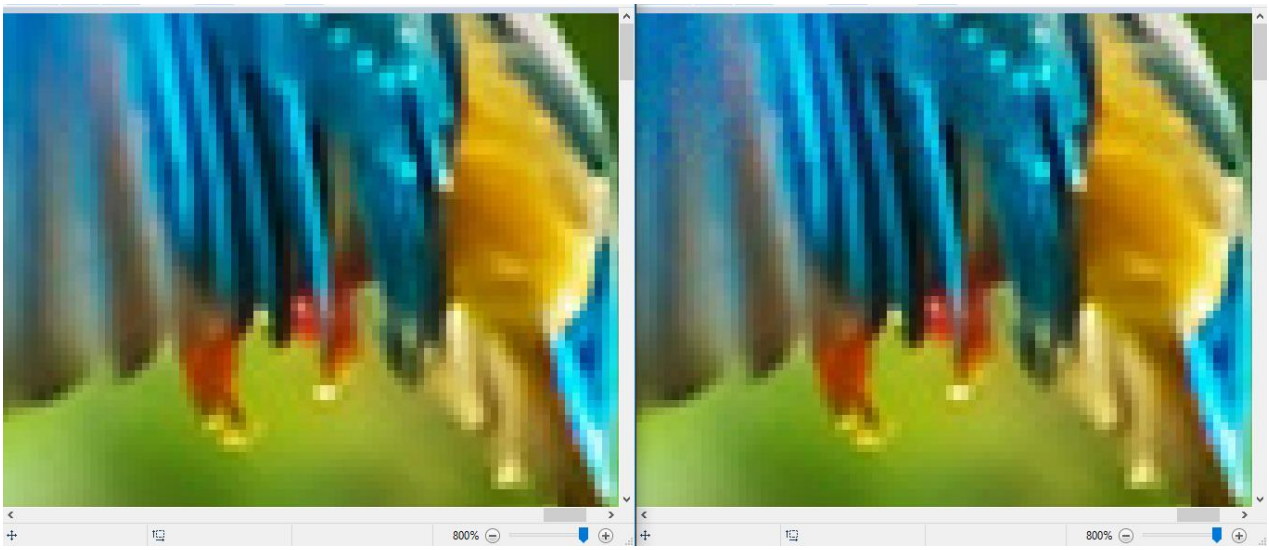


Рис.4.9 Незаповнений (зліва) та заповнений (справа) контейнер №2 при збільшенні у 8 разів. Фрагмент №2

c) В даному прикладі використовується контейнер №3 та секретне зображення №3.

В якості контейнера використовується зображення розміром 800x800 та глибиною кольору: 24 біти. Воно містить лише одну помітну деталь та однотонний фон білого кольору, різкі переходи.

На рис. 4.10 зображено незаповнений контейнер, на рис. 4.11 зображено заповнений контейнер, на рис. 4.12 - секретне зображення, яке було вбудовано, а потім відновлено. Розмір секретного повідомлення становить 24,1 КВ.

Під час проведення опитування у двох людей з десяти виникли підозри стосовно заповненого контейнера.

На рис.4.13 наведено порівняння першого фрагменту незаповненого контейнера №2 (з рис.4.10) та заповненого контейнера №2 (з рис.4.11) при збільшенні у 8 разів. При такому збільшенні можна легко помітити, що заповнений контейнер містить спотворення.

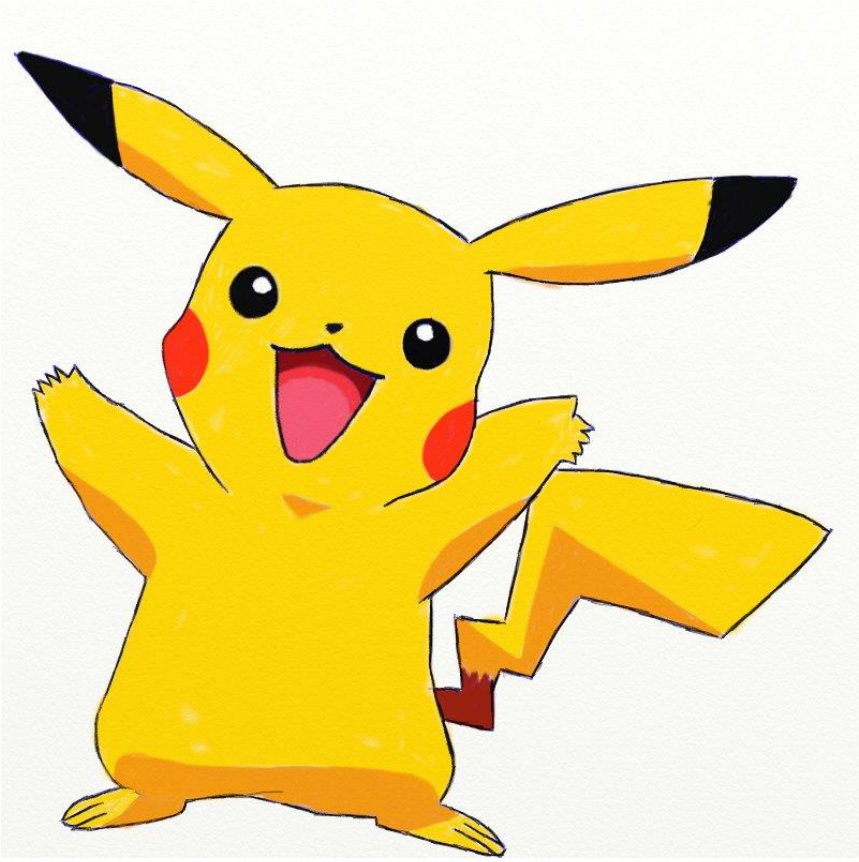


Рис. 4.10 Незаповнений контейнер №3

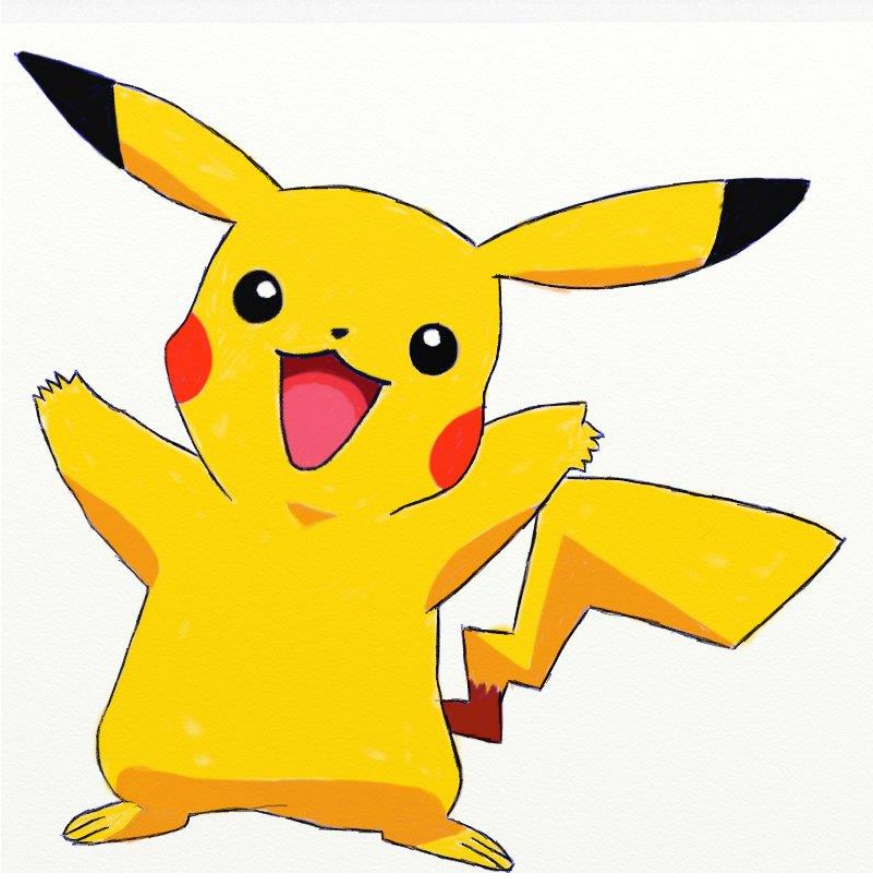


Рис. 4.11 Заповнений контейнер №3

Рис. 4.12 Секретне зображення №3

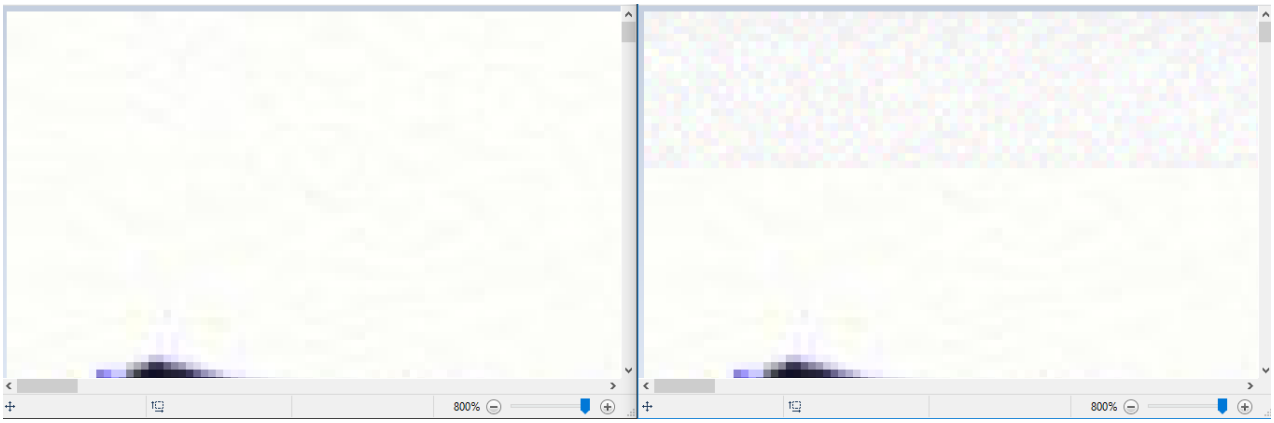


Рис.4.13 Незаповнений (зліва) та заповнений (справа) контейнер №3 при збільшенні у 8 разів.

4.2 Можливості застосування та подальшого розвитку покращеного методу

Зважаючи на проаналізовані у п.1.4 завдання та можливості застосування стеганографії, очевидно, що представлений модифікований метод найкраще підходить для реалізації класичного завдання стеганографії - ППД.

Як видно з п.4.1, на зображеннях певного типу (з різкими переходами та однотонними областями) можна помітити (зазвичай при великому збільшенні) спотворення, що виникають при вбудовуванні секретних даних.

Ці спотворення не є великими, їх вдається помітити лише тому, що секретні дані вбудовуються у пікселі зображення-контейнера підряд.

Щоб вирішити цю проблему, можна використати принцип широкосмугових методів стеганографії - спробувати "розчинити" секретне повідомлення в контейнері. У запропонованому методі для цього достатньо вбудовувати секретні дані рівномірно по всьому контейнеру, а не послідовно.

4.3 Вибір засобів реалізації покращеного методу стеганографії

Мова програмування C#

Для виконання задачі, поставленої в рамках даного дипломного проекту, необхідно було вирішити питання щодо вибору мови програмування. Вибір поставав між об’єктно-орієнтованими мовами, оскільки можливості, які надає об’єктно-орієнтоване програмування, якнайкраще підходять для вирішення поставлених задач.

Мова програмування C# виникла в 2000 році, і була розроблена компанією Microsoft. C# розроблювалась під платформу .Net.

Автори *C#* прагнули створити мову, що поєднує простоту і виразність сучасних об’єктно-орієнтованих мов (на кшталт *Java*) з багатством можливостей і потужністю C++. За словами Андерса Хейлсберга, одного із творців мови, C# запозичив більшість своїх синтаксичних конструкцій з C++. Зокрема, в ньому присутні такі зручні типи даних, як структури та перерахування (інший нащадок C++ – Java – позбавлений цих елементів, що створює певні незручності при програмуванні). Синтаксичні конструкції C# успадковані не тільки від C++, але і від Visual Basic. Наприклад, в C#, як і в Visual Basic, використовуються властивості класів. Як і C++, C# дозволяє виконувати перевантаження операторів для створених типів (Java не підтримує ні ту, ні іншу можливість). *C#* – це фактично гібрид різних мов. При цьому C# синтаксично не менш (якщо не більше) чистий, ніж Java, так само простий, як Visual Basic, і володіє практично тією ж потужністю і гнучкістю, що і C++.

Переваги та особливості мови C# для реалізації поставленої задачі:

- повний і добре визначений набір основних типів;
- вбудована підтримка автоматичної генерації XML-документації; автоматичне звільнення динамічно розподіленої пам’яті;
- можливість позначення класів і методів атрибутами, визначених користувачем. Це може бути корисно при документуванні і здатне впливати на процес компіляції (наприклад, можна позначити методи, які повинні компілюватися тільки в налагоджувальному режимі);
- повний доступ до бібліотеки базових класів .NET, а також легкий доступ до Windows API (якщо це дійсно необхідно);
- покажчики та прямий доступ до пам’яті, якщо вони необхідні. Однак мова розроблена таким чином, що практично у всіх випадках можна обійтися і без цього;
- підтримка властивостей і подій в стилі *VB*;
- проста зміна ключів компіляції. Дозволяє отримувати виконувані файли або бібліотеки компонентів .NET, які можуть бути викликані іншим кодом так само, як елементи керування ActiveX (компоненти COM);
- можливість використання C# для написання динамічних web-сторінок ASP .NET.

При реалізації розробленого ПЗ використовувались наступні компоненти (namespaces) із .NET Framework Class Library:

- System.Drawing

Простір імен System.Drawing містить типи, що підтримують базові графічні функції GDI+. Дочірні простори імен підтримують більш складні функції двомірної і векторної графіки, додаткові функції обробки зображень, а також служби, пов'язані з друком і тд.. Дочірні простори імен також містять типи, які розширюють логічні і графічні можливості призначеного для користувача інтерфейсу під час розробки.

У розробленому ПЗ було використано класи дочірнього простору імен System.Drawing.Imaging, який містить розширені функції для роботи із зображеннями GDI+.

- System.IO

Даний прості імен містить класи, що підтримують введення і виведення, включаючи можливості читання і запису даних в потоках як синхронно, так і асинхронно, стиснення даних в потоках, створення і використання ізольованих сховищ, зіставлення файлів логічним адресним просторам додатків, зберігання різних об'єктів даних в одному контейнері.

- System.Linq

Простір імен System.Linq містять типи, які підтримують запити, які використовують інтегрований мову запитів (LINQ). Це включає типи, які представляють запити як об'єкти в деревах виразів.

- System.Runtime.InteropServices

Даний простір імен містять типи, які підтримують взаємодію програми з загальною мовою середовища виконання, а також типи, що включають такі функції, як кешування даних додатків, розширене керування виключеннями, активація програм у доменах програм, COM-взаємодію, розподілені додатки, серіалізація та десеріалізація.

З даного простору імен було використано клас Marshal. Він містить набір методів розподілу некерованої пам'яті, копіювання некерованих блоків пам'яті та перетворення керованих типів у некеровані (і навпаки), а також інших різноманітних методів, що використовуються при взаємодії з некерованим кодом.

Середовище розробки MS Visual Studio 2015

Окрім мови програмування також потрібно було обрати і середовище програмування. Так як мовою програмування обрано C#, то середовищем розробки доцільно було обрати Microsoft Visual Studio, яка являє собою інтегроване середовище розробки з можливостями створення як консольних

додатків, так і додатків з графічним інтерфейсом та підтримкою платформи .Net.

Microsoft Visual Studio 2015 Community – великий набір засобів управління циклом життя програми для забезпечення якості результатів від етапу проектування до розгортання. При створенні нових проектів або удосконаленні існуючих додатків Visual Studio 2015 дозволяє максимально спростити процес завдяки підтримці різних платформ і технологій, включаючи хмарні і паралельні обчислення.

Як при створенні нових рішень, так і при доопрацюванні існуючих, можливо реалізувати своє бачення за допомогою потужних інструментів створення прототипів, проектування архітектури та розробки, які дозволяють розробляти програми для всіляких платформ і технологій, таких як обробка даних в хмарі і паралельна обробка даних. Розширені можливості координування спільної діяльності поряд з інтегрованими інноваційними інструментами тестування і налагодження забезпечать підвищення продуктивності групи і створення високоякісних і недорогих рішень.

Можливості та переваги Visual Studio 2015:

- потужні інструменти створення прототипів, редагування та візуального дизайну;
- поліпшені засоби аналізу коду та налагодження;
- простота за рахунок інтеграції. Це просте інтегроване середовище дозволяє розробникам застосовувати наявні навички для моделювання, написання коду, налагодження, тестування та розгортання всіляких типів додатків;
- потужні інструменти для управління проектами, обслуговування вихідного коду, виявлення та усунення дефектів. Використання ручного та автоматизованого тестування в поєднанні з поліпшеними інструментами налагодження як при розробці, так і при тестуванні.

Visual Studio 2015 була представлена 20 червня 2015 року. Суттєвою зміною стала підтримка багатьох цільових платформ: окрім базової Windows з'явилась можливість будувати проекти для IOS та Android. Для розробників комп'ютерних ігор була додана підтримка фреймворку Unity. Був оновлений механізм автентифікації: користувач під час запуску Visual Studio синхронізується з єдиним аккаунтом Microsoft.

Допоміжні інструменти, що активно використовувалися під час розробки: ReSharper, GIT.

Для покращення якості написання коду було використано додаток ReSharper. Він є поширеним інструментом для підвищення продуктивності роботи, що дозволяє істотно збільшити функціональність Microsoft Visual Studio. Додаток розроблений компанією JetBrains. Тисячі .NET розробників по всьому світу використовують ReSharper для перевірки коду, автоматизації рефакторингу та одержання допомоги в написанні якісного програмного коду.

Він здійснює миттєвий статичний аналіз коду (без потреби компіляції), передбачає додаткові засоби автодоповнення, навігації, пошуку, виділення синтаксису, форматування, оптимізації та генерації коду, надає близько 40 автоматизованих рефакторингів, спрощує модульне тестування в середовищах MSTest та NUnit.

System Version Control (SVC) — система контролю (управління) версій; програмне забезпечення для полегшення роботи зі змінною інформацією.

Ситуація, в якій електронний документ за час свого існування зазнає ряд змін, досить типова. При цьому часто буває важливо мати не тільки останню версію, але і кілька попередніх. У найпростішому випадку можна просто зберігати кілька варіантів документа, нумеруючи їх відповідним чином. Такий спосіб є неефективним (доводиться зберігати кілька практично ідентичних копій), вимагає підвищеної уваги і дисципліни і часто веде до помилок, тому в такій ситуації доцільно використовувати SVC.

Система управління версіями дозволяє зберігати кілька версій одного і того ж документа, при необхідності повертатися до попередніх версій, визначати, хто і коли зробив ту чи іншу зміну, та багато іншого.

При написанні розробленого ПЗ було використано розподілену систему контролю верій Git.

4.4 Складові програмного рішення

Розроблені програмні модулі

У розробленому ПЗ можна виділити декілька програмних модулів, що виконують певний набір функцій:

- *Модуль Аналізу (Клас Analize)*

Дозволяє оцінювати розміри вхідних файлів (щоб визначити, чи можливе приховування зображень).

Приклади методів класу *Analize*:

bool IsStegoImageProvided(string path);

bool IsSecretFileProvided(string path);

bool IsSecretFileLessThanCoverImage(int secretDataLength, int coverImageLength, double coefizzient);

bool IsSudokuMatrixValid(string content);

і тд.

- *Модуль генерації стегоключа (судоку матриці) за паролем KeyGenerator*

Даний алгоритм реалізовано відповідно до опису п.3.7.

Приклади методів класу *KeyGenerator:*

int[,] GetKey(string password);

- *Модуль генерації судоку матриці SudokuGenerator*

Призначений для генерації матриці судоку, дозволяє виконувати перевірку коректності судоку матриці, базуючись на правилах, описаних у п.3.1.

Приклади методів класу *SudokuMatrixGenerator*:

int[n,n] GenerateSudokuMatrix();

void SwapRowsArea();

void SwapColumsArea();

void SwapRowsSmall();

void Transposing();

void SwapColumsSmall();

bool IsSudokuMatrixValid(int[n,n] matrix);

і тд.

- *Модуль перетворення зображень SteganographyWorker*

Дозволяє закодувати та розкодувати зображення на основі алгоритмів, описаних у 3.5, 3.6, використовуючи багато допоміжних методів, реалізованих у модулі *Helpers*, для здійснення даних операцій.

Приклади методів класу *SteganographyWorker:*

Головні методи класу (з модифікатором доступу «public»):

string Encrypt(int[n,n] sudokuMatrix, byte[] secrectBytesToEncode, coverImage);

string Decrypt(int[n,n] sudokuMatrix, Image modifiedCoverImage);

Деякі допоміжні методи (з модифікатором доступу «private»):

SudokuCoordinate FindNearestCoordinate(int secretNumber, int initialXCoord, int initialYCoord);

та інші.

Розробка даного ПЗ включала активне використання принципів SOLID. Термін "SOLID" є акронімом для набору практик проектування програмного коду і побудови гнучких й адаптивних програм.

Використання принципів SOLID дозволить в майбутньому легко розширювати функціонал програми, а використання патерна MVP – застосовувати ASP.NET MVC, Web API, або WPF замість WindowsForms.

Для максимальної зручності при розширенні функціоналу пропонується покрити більшу частину коду програми unit-тестами. Вони необхідні також для того, щоб захистити код від згубних змін, що можуть виникати при модифікації розроблених бібліотек (Class Library).

Інтерфейс розробленого рішення

Інтерфейс програми складається із головної форми *MainWindow* з двома вкладками: Encryption та Decryption.

Вкладка Encryption дозволяє задати зображення-контейнер, файл секретного повідомлення, встановити пароль і виконати шифрування (вбудовування) даних. Результатом цього процесу є створення заповненого контейнера.

Вкладка Decryption дозволяє задати заповнене зображення-контейнер, пароль і виконати дешифрування (відновлення) інформації. Результатом цього процесу є створення файлу із секретними даними.

Для взаємодії програми з файлами використовуються стандартні файлові діалогові вікна, а для сповіщення користувачів (наприклад, про помилки або про успішне виконання операцій, з повідомленням результатів) використовуються стандартні діалогові вікна.

4.5 Висновки до розділу

Для підтвердження на практиці покращень методу стеганографії з використанням матриці судоку було розроблено ПЗ, яке дозволяє виконувати шифрування, дешифрування за допомогою даного методу.

У цьому розділі проаналізовано результати використання даного методу на практиці, наведено можливості подальшого розвитку даного методу. Для оцінки помітності спотворень заповнених контейнерів було проведено опитування.

На основі проведеного аналізу можна зробити висновок, що модифікований метод володіє доволі високою стійкістю до візуальних атак.

ВИСНОВКИ

У даній магістерській дисертації проведено огляд методів стеганографічного приховування даних. Детально розглянуто якісні та кількісні характеристики стеганографічних систем. Описано завдання та практичне застосування стеганографії.

Розвиток мережі Інтернет призводить до збільшення обсягів інформації, що передається, обробляється та зберігається. А це створює підґрунтя для активного використання стеганографії. Аналіз досліджень і публікацій показав, що найпопулярнішими методами стеганографії є ті, що використовують у ролі контейнера зображення.

Проведений аналіз також показав, що однією з ключових проблем стеганографії є питання оптимального використання стегоконтейнера, оскільки часто виникає потреба у передачі даних великого обсягу, а проаналізовані стегосистеми не мають такої можливості.

При роботі з даними великого обсягу важливим завданням є прискорення процесів шифрування, дешифрування інформації.

Тому для дослідження було обрано метод на основі матриці судоку, оскільки він дозволяє приховувати дані довільного розміру (є лише вимоги щодо співвідношення об’єму між контейнером та секретним зображенням), а використовуваний ключ володіє високою стеганографічною стійкістю. Отримані в процесі дослідження результати дали змогу розробити покращений метод стеганографії з використанням матриці судоку.

Модифікований метод відрізняється від існуючого покращенням якісних показників стегосистеми - пропускної здатності (місткість стегоконтейнера збільшується в три рази в порівнянні з класичним методом) та складності вбудовування і вилучення секретного повідомлення (прискорюються процеси шифрування, дешифрування даних).

Іншою відомою проблемою сучасних стеганографічних методів є використання великих ключів, що заставляє користувачів зберігати їх у вигляді

файлів. Тому важливим завданням постало приведення ключа до такого вигляду, щоб його можна було просто пам’ятати. Тому в даній роботі запропоновано спосіб генерації стегоключа (матриці судоку) за паролем, що дозволяє помітно спростити для користувача використання даного методу стеганографії.

В ході роботи було розроблено систему із застосуванням представленого покращеного методу та проаналізовано результати роботи.

Для оцінки непомітності вбудовування секретних даних було проведено опитування, яке підтвердило що даний метод володіє доволі високою стійкістю до візуальних атак.

Розроблене ПЗ є комплексним вирішення задачі приховування даних.

Для реалізації поставлених задач було використано мову програмування C#.

Розробка виконана відповідно до вимог Завдання на магістерську дисертацію.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кузнецов О. О. К89 Стеганографія: навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. - Х.: Вид. ХНЕУ, 2011. - 232с. [Електронний ресурс]. Режим доступу: http://repository.hneu.edu.ua/jspui/bitstream/123456789/2289/1/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F.pdf. Дата доступу: квітень 2018.
2. В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко. Метод вбудовування стегоповідомлення на основі ключового елемента / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко. // Захист інформації. 2014. С. 53-58.
3. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. - Київ: МК-Пресс, 2006. – 288с.
4. Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації / Вовк О.О. – Харків, 2016 – 177с.
5. Стеганография в XXI веке. Цели. Практическое применение. Актуальность//Хабрахабр. Дата оновлення: 15.03.2015. [Електронний ресурс]. Режим доступу: https://habrahabr.ru/post/253045/. Дата доступу: квітень 2018.
6. Худьо В.Д., Моделювання стійкої стегофонічної системи із заданими характеристиками мережі / В.Д. Худьо // Тернопіль – 2017. – 98с.
7. Sanmitra I., Shivananda P., Shrikant B., Usha B, Image Steganography using Sudoku Puzzle for Secured Data Transmission // International Journal of Computer Applications (0975 – 888) Volume 48– No.17, June 2012
8. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М.: СОЛОН-Пресс, 2002. – 261с.
9. Аграновский А.В., Девянин П.Н., Хади Р.А. / Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. - 152с.
10. К оценке эффективности защиты акустической (речевой) информации / Хорев А.А., Макаров Ю.К. –Специальная техника, 2000.– 46–56с.

11. Введение в компьютерную стеганографию / Хорошко В.А., Шелест М.Е. – К., 2002. – 140 с.
12. Кінзерявий О.М. Стеганографічні методи приховування даних увекторні зображення, стійкі до активних атак на основі афінних перетворень / О.М. Кінзерявий // Київ - 2015
13. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. 2-е изд. / Рябко Б. Я., Фионов А. Н. // М.: Горячая линия - Телеком, 2013. 232 с.
14. Шелест М.Є., Андреев В.1. Комп'ютерна стеганографія та ЇЇ можливості / М.Є. Шелест, В.1. Андреев // Сучасна спеціальна техніка № 1 (24), 2011. С.97-104 [Електронний ресурс]. Режим доступу: http://elar.naiau.kiev.ua/bitstream/123456789/2200/1/%D0%A8%D0%B5%D0%BB%D0%B5%D1%81%D1%82%20%D0%9C.%20%D0%84..pdf. Дата доступу: квітень 2018.
15. PATENTS.COM (complete repository of patents from around the world). [Електронний ресурс]. Режим доступу: http://patents.com/search?top_keyword=steganography&keyword=steganography. Дата доступу: квітень 2018.
16. Патентный поиск в РФ. Новые патенты, заявки на патент библиотека патентов на изобретения. [Електронний ресурс]. Режим доступу http://www.freepatent.ru/. Дата доступу: квітень 2018.
17. База патентів України. [Електронний ресурс]. Режим доступу http://uapatents.com/. Дата доступу: квітень 2018.
18. Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Information Hiding: A Survey (англ.) // Proceedings of the IEEE (special issue). — 1999. — Vol. 87, no. 7. — P. 1062–1078. — DOI:10.1109/5.771065.
19. Громов В.И., Васильев Г.А. // Энциклопедия безопасности. 3-е издание. // Москва - 2007 р.

20. О. В. Генне, ТОВ "Конфідент" журнал "Захист інформації. Конфідент", № 3, 2000, [Електронний ресурс]. Режим доступу: http://easy-code.com.ua/2010/11/osnovni-polozhennya-stenografi%D1%97/. Дата доступу: квітень 2018.
21. Simmons GJ The prisoner's problem and the subliminal channel, Proc. Workshop on Communications Security (Crypto'83), 1984, 51-67.
22. Pfitzmann B. Information Hiding Terminology, in Information Hiding, pringer Lecture Notes in Computer Science, v. 1174, 1996, 347-350.
23. Чунарьова А.В., Потапенко Є.О. Система стеганографічного захисту інформації. [Електронний ресурс]. Режим доступу: http://www.rusnauka.com/10_DN_2013/Informatica/4_132640.doc.htm. Дата доступу: квітень 2018.
24. Suman Chakraborty, Prof. Samir K. Bandyopadhyay Sanmitra I., Steganography Method Based On Data Embedding By Sudoku Solution Matrix. // International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 www.ijesi.org Volume 2 Issue 7. July - 2013. PP.36-42.

ДОДАТКИ

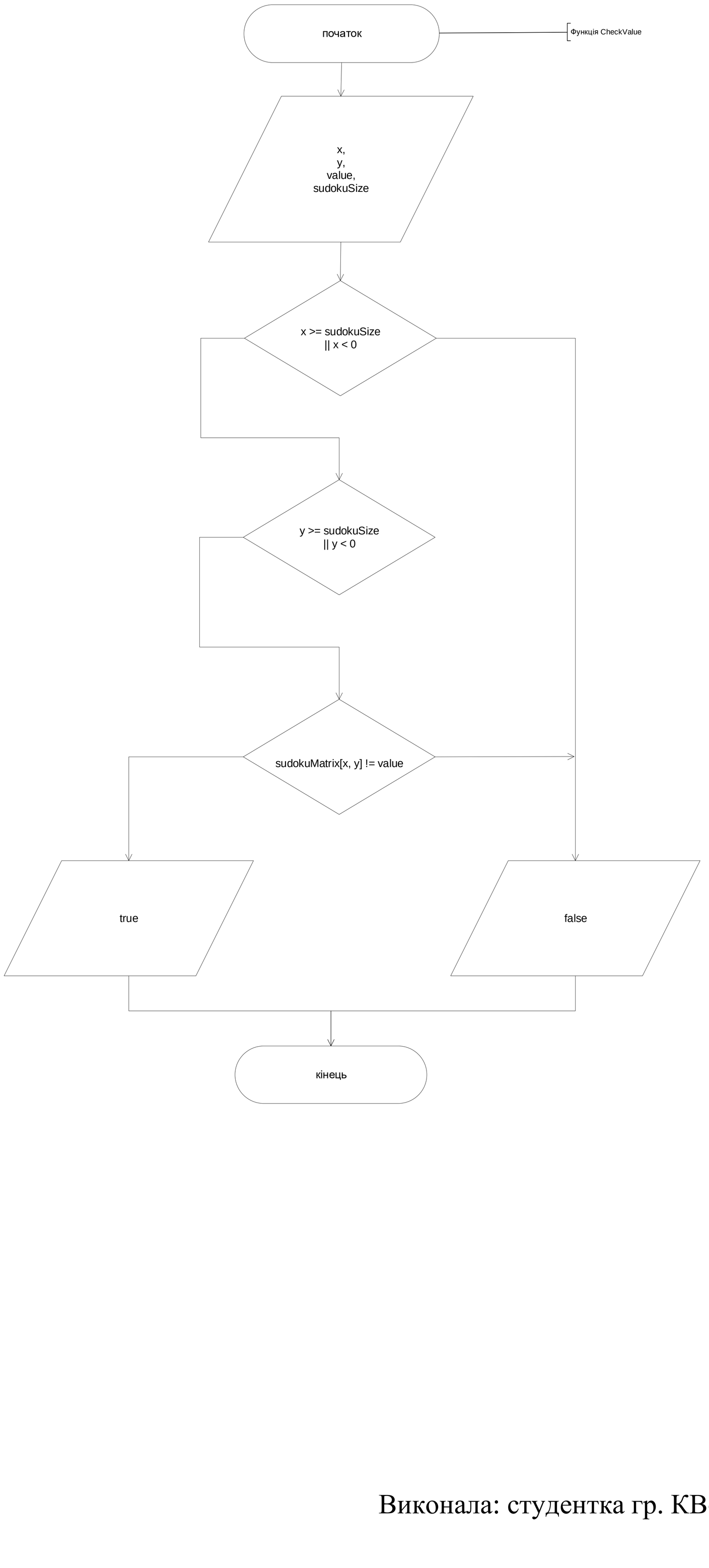
Додаток 1.

Копії графічних матеріалів

Алгоритм перевірки правильності судоку матриці. Схема алгоритму

Виконала: студентка гр. КВ-63м Липка Т.Б.

Перевірка значення в матриці судоку. Схема алгоритму.

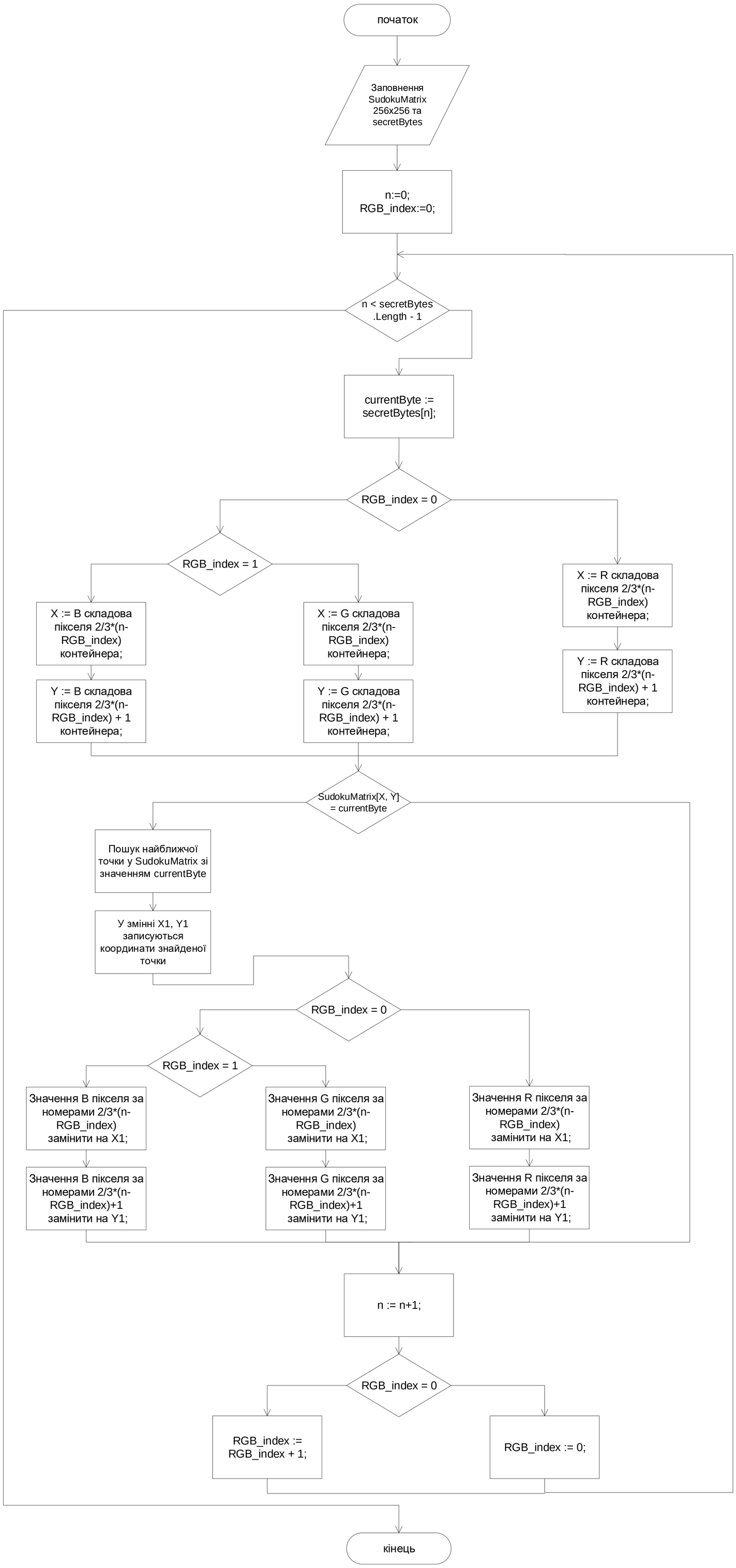


Виконала: студентка гр. КВ-63м Липка Т.Б.

Алгоритм дешифрування. Схема алгоритму.

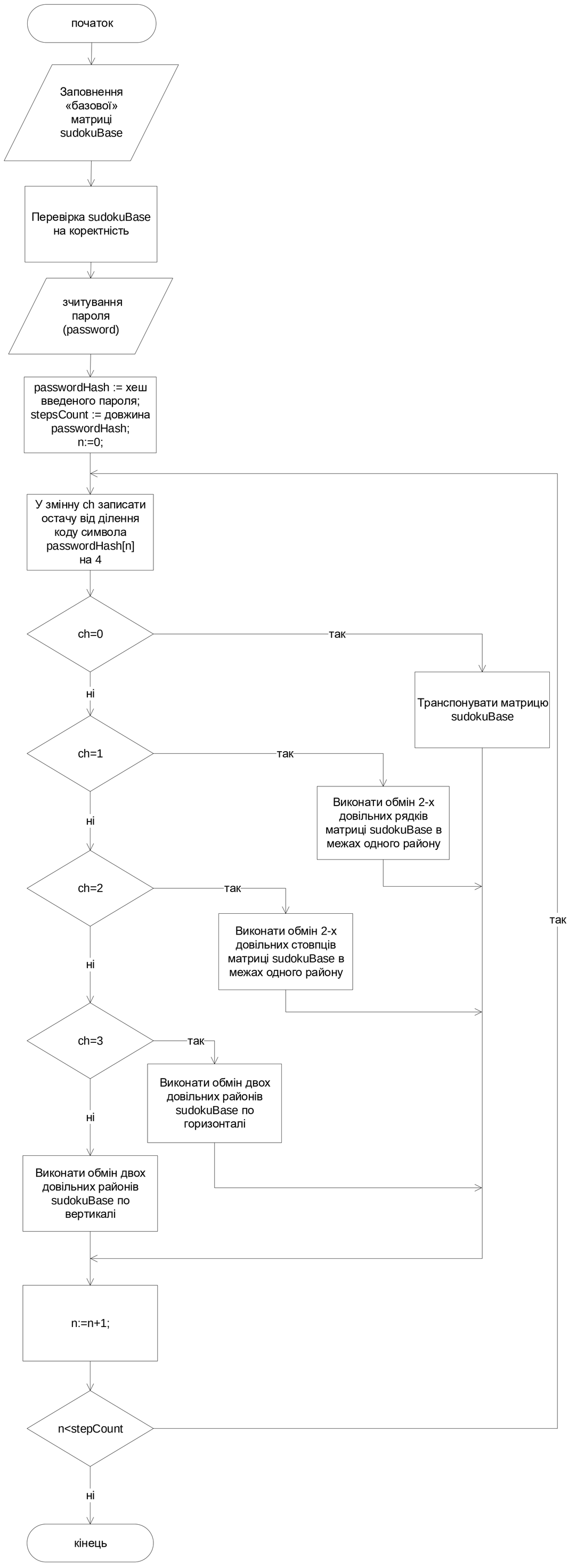
Виконала: студентка гр. КВ-63м Липка Т.Б.

Алгоритм шифрування. Схема алгоритму.



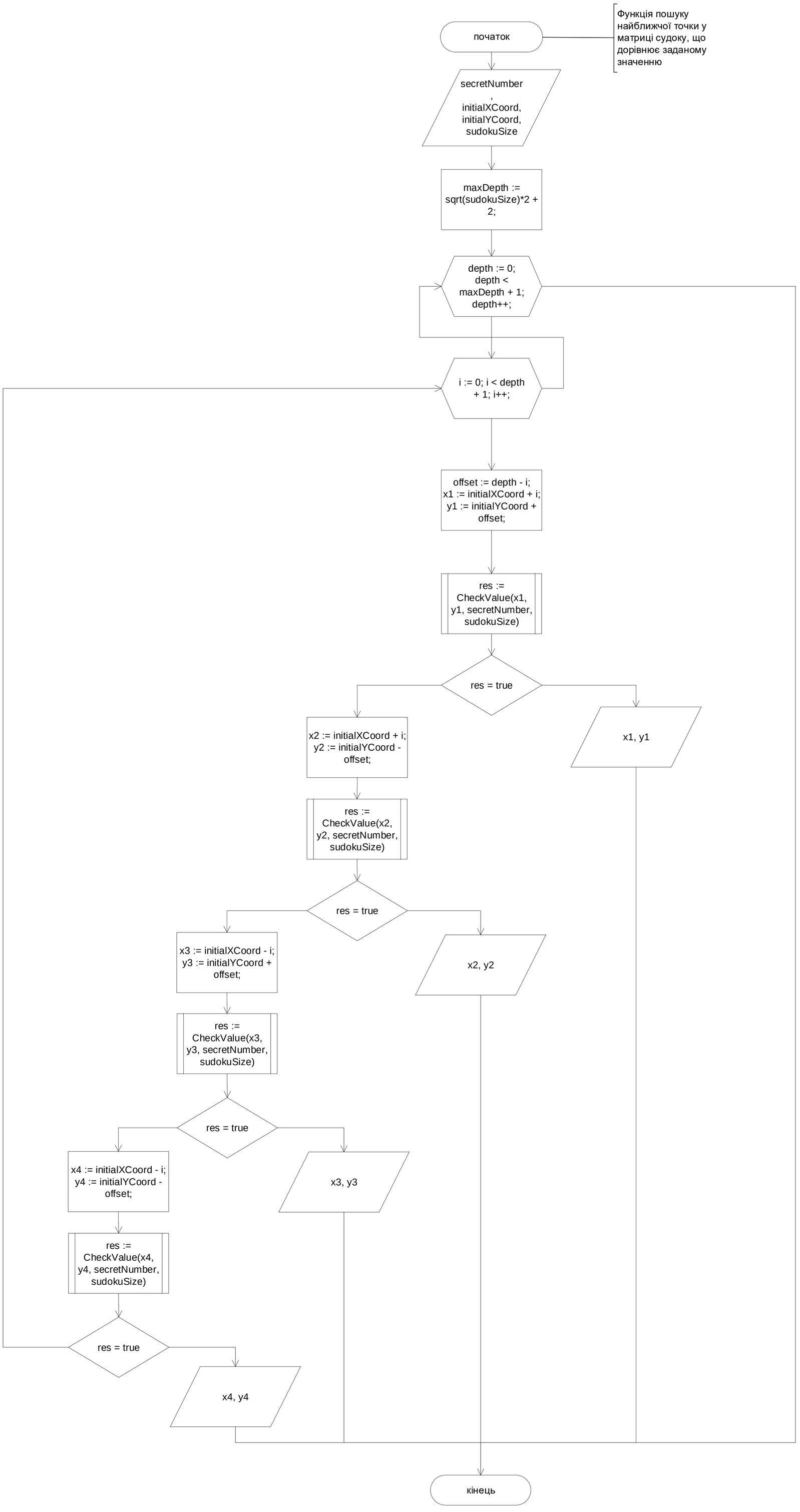
Виконала: студентка гр. КВ-63м Липка Т.Б.

Генерація стегоключа за паролем. Схема алгоритму.



Виконала: студентка гр. КВ-63м Липка Т.Б.

Пошук найближчої точки в матриці судоку. Схема алгоритму.



Виконала: студентка гр. КВ-63м Липка Т.Б.

Додаток 2.

Фрагменти програмного коду

Файл IStegoSystem.cs:

```
namespace SudkuStegoSystem.Logic.Abstract
{
    /// <summary>
    /// Represents stego system functionality in general
    /// </summary>
    public interface IStegoSystem
    {
        /// <summary>
        /// Embeds secret data (from secretDataFilePath file) into container with key
        /// </summary>
        /// <param name="container"></param>
        /// <param name="secretDataFilePath"></param>
        /// <param name="key"></param>
        /// <returns>Path to stogocontainer</returns>
        void Encrypt(string containerFilePath, string secretDataFilePath, string key,
string stegocontainerFilePath = null);

        /// <summary>
        /// Restores secret data from stegocontainer with key
        /// </summary>
        /// <param name="stegocontainer"></param>
        /// <param name="key"></param>
        /// <returns>Path to restored data</returns>
        void Decrypt(string stegocontainerFilePath, string key, string
restoredSecretFilePath = null);
    }
}
```

Файл SudokuStegoSystem.cs:

```
using SudkuStegoSystem.Logic.Abstract;
using SudkuStegoSystem.Logic.Models;
using SudkuStegoSystem.Logic.SudokuMethod.SudokuMatrix;
using System;
using System.Drawing;
using System.Drawing.Imaging;
using System.IO;
using System.Text.RegularExpressions;

namespace SudkuStegoSystem.Logic
{
    /// <summary>
    /// Represents adaptation of SudokuStegoMethod to general stegosystems interface
    /// </summary>
    public class SudokuStegoSystem : IStegoSystem
    {
        private const string KeyRegex = "[a-zA-Z0-9]{6,18}";
        private readonly ISudokuStegoMethod _sudokuStegoMethod;
        private readonly SudokuMatrixFactory _sudokuMatrixFactory;

        public SudokuStegoSystem(ISudokuStegoMethod sudokuStegoMethod,
SudokuMatrixFactory sudokuMatrixFactory)
        {
            _sudokuStegoMethod = sudokuStegoMethod;
            _sudokuMatrixFactory = sudokuMatrixFactory;
        }

        public void Encrypt(string containerFilePath, string secretDataFilePath, string
key, string pathToStegocontainer = null)
        {
            #region checking arguments

            if (!File.Exists(containerFilePath))
            {
                throw new ArgumentException("Container file does not exist.");
            }

            if (!File.Exists(secretDataFilePath))
            {
                throw new ArgumentException("Secret data file does not exist.");
```

```
            }

            if (!Regex.Match(key, KeyRegex).Success)
            {
                throw new ArgumentException("Wrong key format.");
            }

            #endregion

            //ToDo exceptions
            Image containerImage = Image.FromFile(containerFilePath);
            SecretFile secretFileToEncode = new SecretFile(secretDataFilePath);
            SudokuMatrix sudokuKey = GenerateSudokuKey(key);

            Image stegocontainer = _sudokuStegoMethod.Encrypt(containerImage,
secretFileToEncode, sudokuKey);

            string containerFileName = new FileInfo(containerFilePath).Name;
            stegocontainer.Save(Path.Combine(pathToStegocontainer, containerFileName),
ImageFormat.Bmp);
        }

        public void Decrypt(string stegocontainerFilePath, string key, string
pathToRestoreFile = null)
        {
            #region checking arguments

            if (!File.Exists(stegocontainerFilePath))
            {
                throw new ArgumentException("Container file does not exist.");
            }

            //ToDo validate restoredSecretFilePath

            if (!Regex.Match(key, KeyRegex).Success)
            {
                throw new ArgumentException("Wrong key format.");
            }

            #endregion

            Image stegocontainerImage = Image.FromFile(stegocontainerFilePath);
            SudokuMatrix sudokuKey = GenerateSudokuKey(key);

            SecretFile secretFile = _sudokuStegoMethod.Decrypt(stegocontainerImage,
sudokuKey);

            secretFile.Save(pathToRestoreFile);
        }

        #region Private methods

        private SudokuMatrix GenerateSudokuKey(string password)
        {
            return
_sudokuMatrixFactory.GetByPassword(_sudokuStegoMethod.GetExpectedSudokuSize(), password);
        }

        #endregion
    }
}
```

Файл ISudokuStegoMethod.cs:

```
using System.Drawing;
using SudkuStegoSystem.Logic.Models;

namespace SudkuStegoSystem.Logic
{
    public interface ISudokuStegoMethod
```

```
    {
        int GetExpectedSudokuSize();
        Image Encrypt(Image container, SecretFile secretFile, SudokuMatrix sudokuKey);
        SecretFile Decrypt(Image stegocontainer, SudokuMatrix sudokuKey);
    }
}
```

Файл ISudokuMatrixGenerator.cs:

```
namespace SudkuStegoSystem.Logic.SudokuMethod.SudokuMatrix
{
    public interface ISudokuMatrixGenerator
    {
        byte[,] Generate();
    }
}
```

Файл INearestCoordinatesFinder.cs

```
using SudkuStegoSystem.Logic.Models;

namespace SudkuStegoSystem.Logic
{
    public interface INearestCoordinatesFinder
    {
        SudokuCoordinates Find(int valueToFind, SudokuCoordinates initialCoordinates,
byte[,] sudokuMatrix);
    }
}
```

Файл SudokuMatrix.cs

```
using SudkuStegoSystem.Logic.Models;
using SudkuStegoSystem.Logic.SudokuMethod.SudokuMatrix;

namespace SudkuStegoSystem.Logic
{
    /// <summary>
    /// Does actions related to sudoku matrix
    /// </summary>
    public class SudokuMatrix
    {
        private readonly byte[,] _sudokyMatrix;
        private readonly INearestCoordinatesFinder _nearestCoordinatesFinder;
        public int SudokuSize => _sudokyMatrix.GetLength(1);

        public SudokuMatrix(ISudokuMatrixGenerator sudokuMatrixGenerator,
INearestCoordinatesFinder nearestCoordinatesFinder)
        {
            _sudokyMatrix = sudokuMatrixGenerator.Generate();
            _nearestCoordinatesFinder = nearestCoordinatesFinder;
        }

        //or by Coordinates
        public byte this[int x, int y] => _sudokyMatrix[x, y];

        public SudokuCoordinates FindNearestCoordinates(int valueToFind,
SudokuCoordinates initialCoordinates)
        {
            return _nearestCoordinatesFinder.Find(valueToFind, initialCoordinates,
_sudokyMatrix);
        }
    }
}
```

Файл SudokuMatrixFactory.cs

```
namespace SudkuStegoSystem.Logic.SudokuMethod.SudokuMatrix
{
    public class SudokuMatrixFactory
    {
        public Logic.SudokuMatrix GetByPassword(int matrixSize, string password)
        {
```

```
            ISudokuMatrixGenerator matrixGenerator = new
SudokuMatrixGeneratorByPassword(matrixSize, password);
            INearestCoordinatesFinder nearestCoordinatesFinder = new
NearestCoordinatesFinder();

            return new Logic.SudokuMatrix(matrixGenerator, nearestCoordinatesFinder);
        }
    }
}
```

Файл SudokuStegoMethod_256.cs

```
using System;
using System.Linq;
using System.Text;
using System.Drawing;
using System.Drawing.Imaging;
using System.Runtime.InteropServices;
using SudkuStegoSystem.Logic.Helpers;
using SudkuStegoSystem.Logic.Models;

namespace SudkuStegoSystem.Logic
{
    /// <summary>
    /// Just encrypts and decrypts data
    /// </summary>
    public class SudokuStegoMethod_256 : ISudokuStegoMethod
    {
        public int GetExpectedSudokuSize() => 256;

        public Image Encrypt(Image container, SecretFile secretFile, SudokuMatrix
sudokuKey)
        {
            ValidateSudoku(sudokuKey);

            Tuple<byte[], BitmapData> cover =
container.GetByteArrayByImageFile(ImageLockMode.ReadWrite);
            byte[] coverBytes = cover.Item1;
            BitmapData coverBitmap = cover.Item2;
            byte[] secretData = GetSecretBytesToEncode(secretFile);

            if (secretData.Length * 2 >= coverBytes.Length)
            {
                throw new ArgumentException("Cannot encrypt secret data because cover
image is too small.");
            }

            #region Embedding secret data into the container

            for(int i = 0, secretDataIterator = 0;
                i + 1 < coverBytes.Length && secretDataIterator < secretData.Length;
                i += 2, secretDataIterator++)
            {
                byte currentByte = secretData[secretDataIterator];
                SudokuCoordinates initialCoordinates = new
SudokuCoordinates(coverBytes[i], coverBytes[i + 1]);
                SudokuCoordinates nearestCoordinates =
sudokuKey.FindNearestCoordinates(currentByte, initialCoordinates);

                if(initialCoordinates != nearestCoordinates)
                {
                    coverBytes[i] = nearestCoordinates.X;
                    coverBytes[i + 1] = nearestCoordinates.Y;
                }
            }

            #endregion

            Marshal.Copy(coverBytes, 0, coverBitmap.Scan0, coverBytes.Length);
            container.UnlockBits(coverBitmap);
```

```
            return container;
        }

        public SecretFile Decrypt(Image stegocontainer, SudokuMatrix sudokuKey)
        {
            ValidateSudoku(sudokuKey);

            Tuple<byte[], BitmapData> stego =
stegocontainer.GetByteArrayByImageFile(ImageLockMode.ReadOnly);
            byte[] stegoBytes = stego.Item1;
            BitmapData stegoBitmap = stego.Item2;

            #region Extracting secret data

            //decode file length
            var fileLengthValueInByteArray = new byte[4];
            int stegoIterator = 0;
            for (int i = 0; i < 4; stegoIterator += 2, i++)
            {
                fileLengthValueInByteArray[i] = sudokuKey[stegoBytes[stegoIterator],
stegoBytes[stegoIterator + 1]];
            }

            int secretFilePayloadLength =
BitConverter.ToInt32(fileLengthValueInByteArray, 0);

            // decode secret file name length (stored in a 1 byte)
            int secretFileNameLength = sudokuKey[stegoBytes[stegoIterator],
stegoBytes[stegoIterator + 1]];

            //decode file name
            byte[] fileNameBytes = new byte[secretFileNameLength];

            stegoIterator += 2;
            for (int i = 0; i < secretFileNameLength; stegoIterator += 2, i++)
            {
                fileNameBytes[i] = sudokuKey[stegoBytes[stegoIterator],
stegoBytes[stegoIterator + 1]];
            }

            string secretFileName = Encoding.ASCII.GetString(fileNameBytes, 0,
fileNameBytes.Length);

            //decode secret file payload
            byte[] secretFilePayloadBytes = new byte[secretFilePayloadLength];

            for (int i = 0; i < secretFilePayloadLength; stegoIterator += 2, i++)
            {
                secretFilePayloadBytes[i] = sudokuKey[stegoBytes[stegoIterator],
stegoBytes[stegoIterator + 1]];
            }

            #endregion

            stegocontainer.UnlockBits(stegoBitmap);
            return new SecretFile(secretFileName, secretFilePayloadBytes);
        }

        #region Private methods

        private void ValidateSudoku(SudokuMatrix sudokuKey)
        {
            if (sudokuKey.SudokuSize != GetExpectedSudokuSize())
            {
                throw new ArgumentException($"This steganography method works only with
matrix {GetExpectedSudokuSize()}x{GetExpectedSudokuSize()}.");
            }
```

```
            //ToDo mb, other validation
        }

        /// <summary>
        /// Gets bytes to encode by file. FL = 4byte, FNL = 1byte, FN = computed, Payload
= computed
        /// </summary>
        /// <param name="filePath"></param>
        /// <returns></returns>
        private byte[] GetSecretBytesToEncode(SecretFile file)
        {
            byte[] fileLength = BitConverter.GetBytes(file.Payload.Length);//4 bytes

            byte[] fileNameLength = new byte[1] {
BitConverter.GetBytes(file.FileName.Length).First() };//1 byte should be enought
            byte[] fileName = Encoding.ASCII.GetBytes(file.FileName);

            byte[] resultBytes = new byte[4 + 1 + fileName.Length + file.Payload.Length];
            Buffer.BlockCopy(fileLength, 0, resultBytes, 0, fileLength.Length);
            Buffer.BlockCopy(fileNameLength, 0, resultBytes, fileLength.Length,
fileNameLength.Length);
            Buffer.BlockCopy(fileName, 0, resultBytes, fileLength.Length +
fileNameLength.Length, fileName.Length);
            Buffer.BlockCopy(file.Payload, 0, resultBytes, fileLength.Length +
fileNameLength.Length + fileName.Length, file.Payload.Length);

            //Marshal.Copy(ditherBmpData.Scan0, ditherBytes, 0, ditherBytes.Length);

            return resultBytes;
        }

        #endregion
    }
}
```

Додаток 3.

Копії публікацій

***Романкевич В.О.*[1], *Липка Т.Б.*[1]**
[1] *Факультет прикладної математики НТУУ "КПІ ім. Ігоря Сікорського", Київ, Україна*

Модифікація методу стеганографії з використанням матриці судоку

Вступ. Стеганографія - давня і міждисциплінна наука, що активно розвивається. Зокрема, починаючи приблизно з 2008 року нею стали цікавитися не тільки математики-криптографи, а й лінгвісти, філологи і навіть хіміки. [6] На даний момент в США зареєстровано 119 патентів по стеганографії, [2] в Росії - 63, [3] в Україні - 12 [4].

Класичною ціллю стеганографії є прихована передача даних. Вона полягає в передачі інформації таким чином, щоб противник не здогадався про сам факт існування прихованого повідомлення. Окрім цього, її цілями також є: цифрові підписи (Digital Fingerprint), стеганографічні водяні знаки (Stego Watermarking). [6]

Актуальні проблеми. Аналіз останніх досліджень і публікацій [7]- [9] показав, що найбільшу популярність в комп'ютерній стеганографії здобули методи, що використовують у ролі контейнера зображення.

Проведений аналіз також показав, що однією з ключових проблем стеганографії є питання оптимального використання стего-контейнера, оскільки потреба у передачі даних великого обсягу виникає частіше, ніж потреба у передачі даних невеликого обсягу. [8]

При роботі з даними великого обсягу важливим завданням є прискорення процесів шифрування, дешифрування інформації.

Часто сучасні стеганографічні методи використовують великі ключі, що заставляє користувачів зберігати їх у вигляді файлів. В такому випадку існує небезпека у викраденні цих файлів. Тому важливим завданням є приведення ключа до такого вигляду, щоб його можна було просто пам'ятати.

Критеріями оцінки стеганосистем є їхні якісні (пропускна здатність, стійкість, невидимість, захищеність, складність вбудовування і вилучення секретного повідомлення) та кількісні (співвідношення «сигнал/шум» (SNR), якість зображення (IF)) показники. [5] Отже, актуальним є питання покращення цих показників.

Вищевказані критерії є взаємно конкуруючими і не можуть бути оптимальними одночасно. Наприклад, якщо необхідно приховати велике повідомлення, то неможливо вимагати абсолютної невидимості і високої стійкості. Завжди необхідний оптимальний компроміс. [5]

Мета. Метою даної роботи є покращення деяких якісних показників методу стеганографії з використанням матриці судоку. Показниками, що покращуються є:

1. **Пропускна здатність** - кількість бітів секретного повідомлення, які можуть бути передані за допомогою даного методу в стего-контейнері фіксованого розміру.
2. **Складність вбудовування і вилучення** - кількість стандартних операцій, які необхідно виконати для вбудовування і виявлення секретного повідомлення.

Метод стеганографії з використанням матриці судоку. Класична реалізація даного методу передбачає, що контейнер та секретне повідомлення - це зображення у форматі bmp, а ключ - матриця судоку. Метод полягає у модифікації виділених пар пікселів стего-контейнера базуючись на цій матриці.

Даний метод дозволяє закодувати 1 піксель (3 байти) секретного зображення за допомогою 6-ти пікселів (18 байт) контейнера.

Матриця судоку. Квадратна матриця NxN є судоку матрицею, якщо виконуються наступні умови:

- Для заповнення матриці використовується лише заданий набір з N цифр,
- Цифри в межах кожного з рядків унікальні,
- Цифри в межах кожного з стовпчиків унікальні,
- Цифри в межах кожного з районів унікальні (Матриця послідовно ділиться на райони - квадрати зі сторонами $\sqrt{N}$)

Завдяки останньому правилу побудови судоку, така стеганосистема характеризується високою невидимістю (характеристика, що відповідає за неспроможність людського зору виявити стеганографічне повідомлення без використання спеціальних засобів).

Пропонується. Пропонуються модифікації методу стеганографії з використанням матриці судоку:

1. Збільшення розміру ключа - замість стандартної матриці судоку 9x9 використовувати 256x256 та не виконувати її дублювання.
2. Відмова від використання дев'яткової системи числення. Завдяки цьому зникає необхідність виконувати перетворення чисел з десяткової в дев'яткову систему числення та навпаки.
3. Перехід до оперування повними значеннями складових кольору (значення R, G, або B), а не по цифрах, як в існуючих методах.

Завдяки цьому модифікований метод дозволяє закодувати 1 піксель (3 байти) секретного зображення за допомогою 2-х пікселів (6 байт) контейнера.

Висновки. Приховування інформації - актуальна тема на протязі всього часу існування людства. Поширення мережі Інтернет призводить до збільшення обсягів інформації, що передається, обробляється та зберігається. А це створює підґрунтя для активного використання стеганографії.

Аналіз досліджень і публікацій показав, що найпопулярнішими методами стеганографії є ті, що використовують у ролі контейнера зображення. Тому було вивчено і запропоновано модифікацію одного з них - методу стеганографії з використанням матриці судоку.

Модифікований метод відрізняється від існуючого покращенням якісних показників стеганосистеми - пропускної здатності та складності вбудовування і вилучення секретного повідомлення.

Місткість стего-контейнера збільшується у 3 рази. А зникнення необхідності у виконанні перетворень між десятковою та дев'ятковою системами числення і оперування повними складовими кольорів дозволяє прискорити процеси шифрування і дешифрування даних.

Література. **1.** Конахович Г.Ф. Компьютерная стеганография / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: «МК-Пресс», 2006. – 288 с. **2.** http://patents.com/search?top_keyword=steganography&keyword=steganography. **3.** http://www.freepatent.ru/. **4.** http://uapatents.com/. **5.** Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації http://nure.ua/wp-content/uploads/dis_Vovk.pdf. **6.** https://habrahabr.ru/post/253045/. **7.** Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. 2-е изд. / Рябко Б. Я., Фионов А. Н. // М.: Горячая линия - Телеком, 2013. 232 с. **8.** В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко. Метод вбудовування стегоповідомлення на основі ключового елемента / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко. // Захист інформації. 2014. С. 53-58. **9.** Кузнецов О. О. Стеганографія : навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. // – Х. : Вид. ХНЕУ, 2011. – 232с.

УДК 004.056.55

К.т.н. Потапова К.Р., студент Липка Т.Б.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

МЕТОДИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ. МОДИФІКАЦІЯ МЕТОДУ СТЕГАНОГРАФІЇ З ВИКОРИСТАННЯМ МАТРИЦІ СУДОКУ

Abstract

Kateryna R. Potapova, assoc. prof., PhD; Lypka Tetiana, student

Information hiding methods. Modification of Image Steganography using Sudoku Puzzle

This paper is about Image Steganography - the method of hiding the presence of data in cover images. The modification of "Image Steganography using Sudoku Puzzle for Secured Data Transmission" algorithm is proposed.

This paper concerns the task of optimal cover image usage and algorithm performance improving.

Вступ

Поширення мережі Інтернет, зростання популярності хмарних сховищ даних призводить до збільшення обсягів інформації, що передається, обробляється та зберігається. Використовуючи можливості та ресурси мережі Інтернет, можна організовувати різні канали зв’язку, сховища даних.

Наприклад, для військових, розвідувальних цілей необхідно забезпечувати не тільки добре захищені (криптографічно-стійкі) канали зв’язку та сховища, але й приховувати факт наявності секретних даних, щоб зловмисникам було неможливо визначити, які саме файли містять секретну інформацію. Організація такого приховання в каналах передачі або в сховищах даних здійснюється стеганографічними методами захисту інформації. Основна відмінність стеганографії від інших методів захисту інформації, полягає саме у прихованні факту існування секретного повідомлення в іншому, зовсім непримітному об’єкті – контейнері, використовуючи для цього структурні особливості побудови, психо-візуальну надлишковість самого контейнера та властивості органів сприйняття людини.

Аналіз останніх досліджень і публікацій [1-4] показує, що у наукових публікаціях особливу увагу присвячено основним принципам та засобам забезпечення інформаційної безпеки, серед яких важливе місце посідає організація та здійснення прихованого обміну інформації на основі застосування методів комп'ютерної стеганографії [1-4].

Серед останніх досліджень і публікацій варто виділити дослідження, що стосуються аналітичного огляду великої кількості алгоритмів вбудовування, запропонованих за останні роки [2], класифікації стегосистем та методів вбудовування, формального математичного опису та структурної схеми стеганографічної системи захисту інформації на основі теорії секретних систем, проблем цифрової обробки сигналів, що виникають при вбудовуванні інформації, детального дослідження підвищення пропускної здатності стегоканалу, забезпечення стійкості та непомітності вбудовування [2].

Аналіз останніх досліджень і публікацій [1-3] показує, що найбільшу популярність в комп'ютерній стеганографії здобули стеганографічні методи, які використовують у ролі контейнера зображення.

Проведений аналіз показав, що однією з ключових проблем стеганографії є питання оптимального використання стего-контейнера, оскільки потреба у передачі даних великого обсягу виникає частіше, ніж потреба передачі даних невеликого обсягу. [2]

Кожен з пропонованих раніше методів відрізняється своїми якісними характеристиками, проте пошук оптимального співвідношення місткості контейнера і його спотворення триває досі.

При роботі з даними великого обсягу важливим завданням є збільшення швидкості процесів шифрування, дешифрування інформації.

Часто сучасні стеганографічні методи використовують великі ключі, що заставляє користувачів зберігати їх у вигляді файлів. Тому отримувати доступ до секретних даних можна лише при наявності даних файлів. Це створює незручності для користувачів. Варіант збереження ключів у вигляді файлів є також небезпечним, оскільки в такому випадку зловмисник може їх викрасти. Тому актуальним є питання приведення ключа до такого вигляду, щоб його можна було просто пам'ятати.

Мета роботи

Мета роботи полягає в покращенні показників ефективності використання стего-контейнера та прискорення процесів шифрування, дешифрування даних у методі стеганографії з використанням матриці судоку.

Метод стеганографії з використанням матриці судоку

Метод стеганографії з використанням матриці судоку передбачає, що контейнер та секретне повідомлення – це зображення у форматі bmp, а ключ – матриця судоку. Метод полягає у модифікації виділених пар пікселів стего-контейнера базуючись на цій матриці.

Квадратна матриця NxN є судоку матрицею, якщо виконуються наступні умови:

- Для заповнення матриці використовується лише заданий набір з N цифр,
- Цифри в межах кожного з рядків унікальні,
- Цифри в межах кожного з стовпчиків унікальні,
- Цифри в межах кожного з районів унікальні (Матриця послідовно ділиться на райони – квадрати зі сторонами sqrt(N))

Завдяки четвертому правилу побудови судоку, спотворення контейнера виглядають непомітними для людини.

В існуючих методах стеганографії використовується матриця судоку розміром 9x9. Це заставляє під час шифрування та дешифрування виконувати:

- перетворення вмісту судоку-матриці між дев'ятковою та десятковою системами числення, здійснювати її дублювання,
- перетворення значень R, G, B пікселів секретного зображення між дев'ятковою та десятковою системами числення, оперувати цифрами значень R, G, B.

Існуючі методи дозволяють закодувати 1 піксель секретного зображення за допомогою 6-ти пікселів контейнера.

Опис модифікованого алгоритму

В якості контейнера пропонується використовувати зображення у форматі bmp. Ключ – матриця судоку розміром 256x256, числа для заповнення – від 0 до 255. Алгоритм кодування даних зображено на Рис.1.

Після генерації судоку матриці (ключа), можна розпочинати кодування даних. Для цього беремо перший байт секретних даних.

Беремо 2 пікселі картинки-контейнера. Зчитуємо значення у R складових пікселів - вибрані значення слугуватимуть початковою X та Y координатою у матриці судоку розміром 256 на 256.

В матриці шукаємо координати X1, Y1 такі, що найближчі до X, Y, та значення в їхній комірці дорівнює значенню зчитаного байту секретних даних.

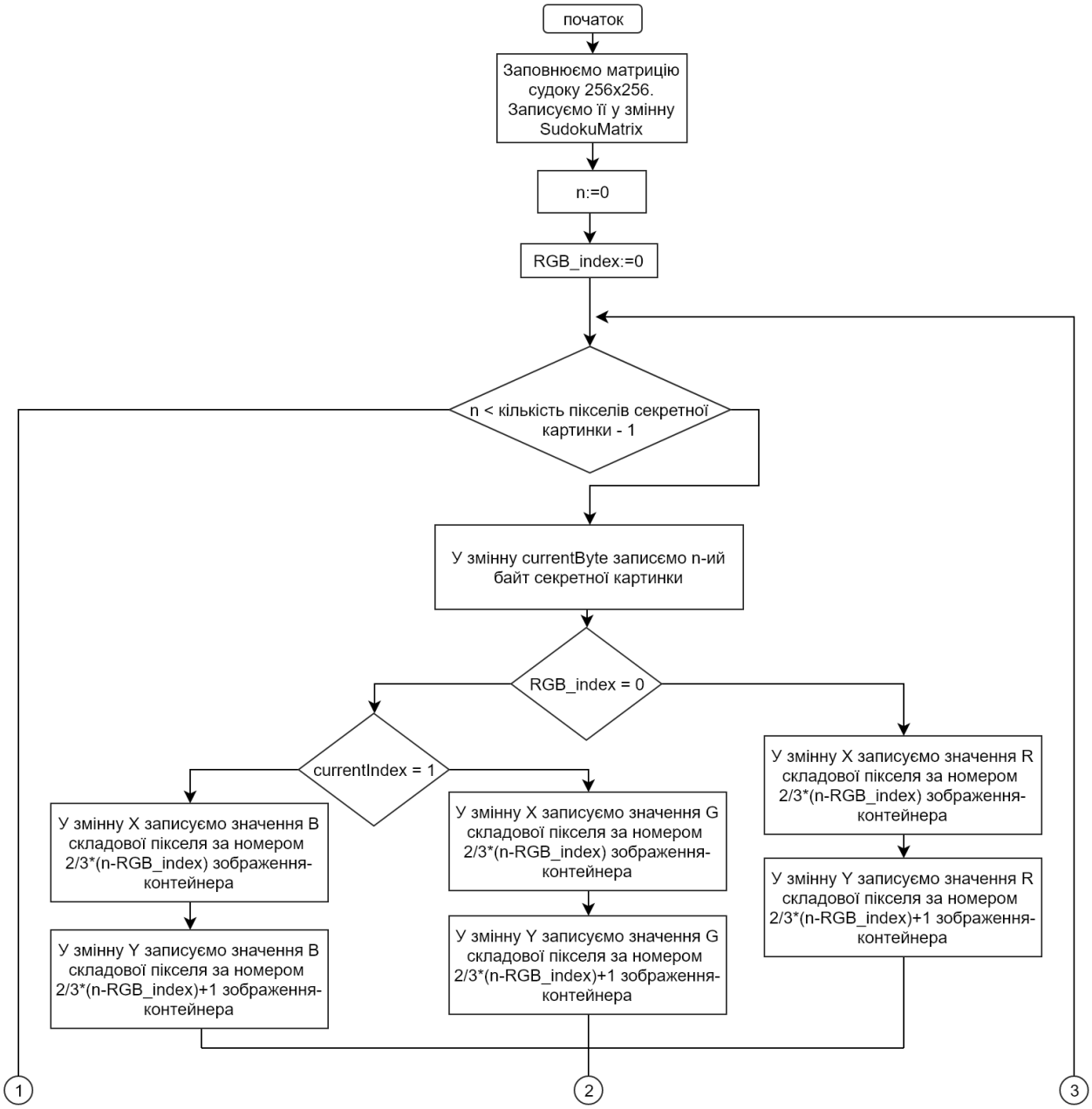


Рис.1. Модифікований алгоритм кодування (частина 1)

Змінюємо значення щойно обраних R складових двох пікселів картинки-контейнера зі значень X, Y на X1, Y1 відповідно.

Аналогічно для другого байту секретних даних використовуємо G складові перших двох пікселів, а для третього – B складові.

Повторюємо такі дії для всіх наступних байтів секретних даних.

Висновки

Пропонуються модифікації методу стеганографії з використанням матриці судоку:

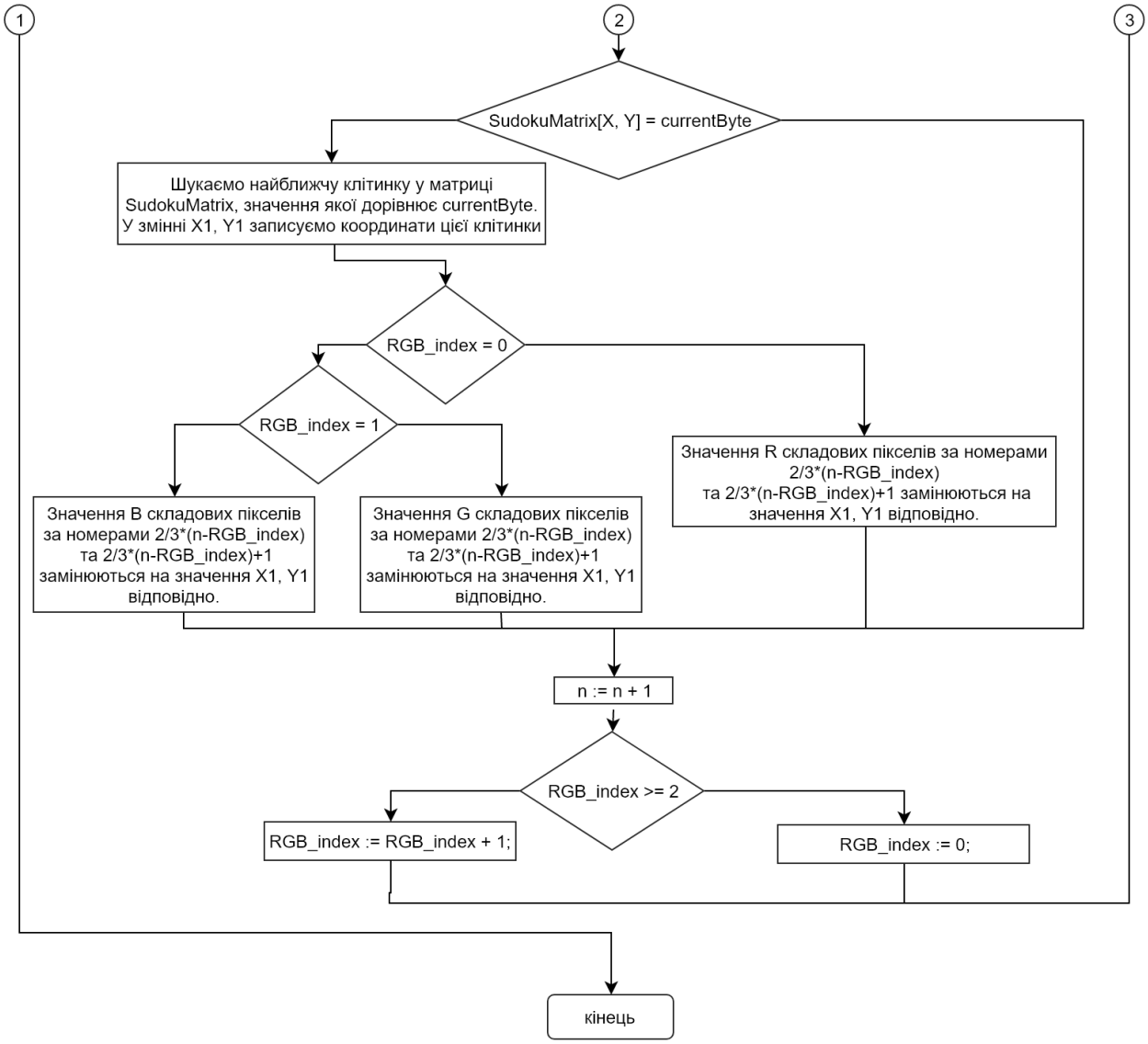


Рис.2. Модифікований алгоритм кодування (частина 2)

1. Збільшення розміру ключа - замість стандартної матриці судоку 9x9 використовувати 256x256 та не виконувати її дублювання.
2. Не виконувати перетворення чисел з десяткової в дев'яткову систему числення та навпаки. Оперувати лише десятковою системою числення.
3. Оперувати повними значеннями складових кольору (значення R, G, або B), а не по цифрах, як в існуючих методах.

Таким чином, модифікований метод дозволяє закодувати 1 піксель секретного зображення за допомогою 2-х пікселів контейнера. Тобто, місткість стего-контейнера збільшується у 3 рази.

А зникнення необхідності у виконанні перетворень між десятковою та дев’ятковою системами числення і оперування повними складовими кольорів дозволяє покращити швидкодію.

Література

1. *Рябко Б. Я., Фионов А. Н.* Основы современной криптографии и стеганографии. 2-е изд. / Рябко Б. Я., Фионов А. Н. // М.: Горячая линия - Телеком, 2013. 232 с.
2. *В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко.* Метод вбудовування стегоповідомлення на основі ключового елемента / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко. // Захист інформації. 2014. С. 53-58.
3. *Кузнецов О. О.* Стеганографія : навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. // – Х. : Вид. ХНЕУ, 2011. – 232с.
4. *Sanmitra I., Shivananda P., Shrikant B., Usha B,* Image Steganography using Sudoku Puzzle for Secured Data Transmission // International Journal of Computer Applications (0975 – 888) Volume 48– No.17, June 2012